

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2002年 6月28日

出 願 番 号

Application Number:

特願2002-189072

[ ST.10/C ]:

[ JP2002-189072 ]

出 願 人

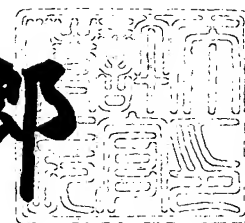
Applicant(s):

インクリメント・ピー株式会社

2003年 2月 7日

特 許 庁 長 官  
Commissioner,  
Japan Patent Office

太田 信一郎



出証番号 出証特2003-3005783

【書類名】 特許願

【整理番号】 57P0010

【提出日】 平成14年 6月28日

【あて先】 特許庁長官 殿

【国際特許分類】 H04L 12/00

【発明者】

    【住所又は居所】 東京都目黒区下目黒1丁目7番1号 インクリメント・  
                                ピー株式会社内

    【氏名】 柴田 紀正

【特許出願人】

    【識別番号】 595105515

    【氏名又は名称】 インクリメント・ピー株式会社

【代理人】

    【識別番号】 100083839

    【弁理士】

    【氏名又は名称】 石川 泰男

    【電話番号】 03-5443-8461

【手数料の表示】

    【予納台帳番号】 007191

    【納付金額】 21,000円

【提出物件の目録】

    【物件名】 明細書 1

    【物件名】 図面 1

    【物件名】 要約書 1

    【包括委任状番号】 9814643

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 通信機器認証システム、通信機器認証方法、通信機器認証サーバ装置、通信機器認証用プログラムおよび情報記録媒体

【特許請求の範囲】

【請求項 1】 通信端末装置から通信手段を介して入力されるユーザ特定情報に基づいて前記通信端末装置を使用するユーザに対して認証を行い、その認証結果に基づいてサーバ装置から前記通信端末装置にデータを供給する通信機器認証システムであって、

前記通信端末装置から送信されるユーザ特定情報を認証し、当該ユーザ特定情報に基づいて第 1 のキー情報を生成して前記サーバ装置から前記通信端末装置に送信する第 1 の認証手段と、

前記通信端末装置から送信される前記第 1 のキー情報を認証し、当該第 1 のキー情報に基づいて前記データに対してアクセスする第 2 のキー情報を生成して前記サーバ装置から前記通信端末装置に送信する第 2 の認証手段と、

前記通信端末装置から前記サーバ装置への前記第 2 のキー情報に基づくアクセスを所定時間内のみ許可するアクセス許可手段と、

を備えたことを特徴とする通信機器認証システム。

【請求項 2】 請求項 1 に記載の通信機器認証システムにおいて、

前記第 1 のキー情報が前記サーバ装置に対してアクセスするアクセスキーであって、前記第 2 のキー情報がセッションキーであることを特徴とする通信機器認証システム。

【請求項 3】 請求項 1 または 2 に記載の通信機器認証システムにおいて、

前記第 1 の認証手段は、前記通信端末装置とは別の通信端末装置を用いて前記ユーザ特定情報が送信された場合、当該ユーザ特定情報に基づいて生成するアクセスキーを前記アクセスキーと同一のアクセスキーとして付与することを特徴とする通信機器認証システム。

【請求項 4】 請求項 1 に記載の通信機器認証システムにおいて、

前記通信端末装置には、予め設定された装置識別情報が入力されており、この装置識別情報を前記ユーザ特定情報とともに前記サーバ装置で受信可能としたこ

とを特徴とする通信機器認証システム。

【請求項 5】 請求項 1 に記載の通信機器認証システムにおいて、  
前記サーバ装置により生成された第 2 のキー情報を認証する第 3 の認証手段を、  
前記サーバ装置とは別のサーバ装置に設けたことを特徴とする通信機器認証システム。

【請求項 6】 請求項 1 または 5 に記載の通信機器認証システムにおいて、  
前記別のサーバ装置は、前記第 2 のキー情報を取得した時刻とアクセス許可残り時間に基づいて前記データに対してアクセスする時間を設定することを特徴とする通信機器認証システム。

【請求項 7】 通信端末装置から通信手段を介して入力されるユーザ特定情報に基づいて前記通信端末装置を使用するユーザに対して認証を行い、その認証結果に基づいてサーバ装置から前記通信端末装置にデータを供給する通信機器認証方法であって、

前記通信端末装置から送信されるユーザ特定情報を認証し、当該ユーザ特定情報に基づいて第 1 のキー情報を生成して前記サーバ装置から前記通信端末装置に送信する第 1 の認証工程と、

前記通信端末装置から送信される前記第 1 のキー情報を認証し、当該第 1 のキー情報に基づいて前記データに対してアクセスする第 2 のキー情報を生成して前記サーバ装置から前記通信端末装置に送信する第 2 の認証工程と、

前記通信端末装置から前記サーバ装置への前記第 2 のキー情報に基づくアクセスを所定時間内のみ許可するアクセス許可工程と、

を備えたことを特徴とする通信機器認証方法。

【請求項 8】 請求項 7 に記載の通信機器認証方法において、  
前記第 1 のキー情報が前記サーバ装置に対してアクセスするアクセスキーであって、前記第 2 のキー情報がセッションキーであることを特徴とする通信機器認証方法。

【請求項 9】 請求項 7 または 8 に記載の通信機器認証システムにおいて、  
前記第 1 の認証工程は、前記通信端末装置とは別の通信端末装置を用いて前記ユーザ特定情報が送信された場合、当該ユーザ特定情報に基づいて生成するアク

セスキーを前記アクセスキーと同一のアクセスキーとして付与することを特徴とする通信機器認証方法。

【請求項 1 0】 請求項 7 に記載の通信機器認証方法において、

前記通信端末装置には、予め設定された装置識別情報が入力されており、この装置識別情報を前記ユーザ特定情報とともに前記サーバ装置で受信可能としたことを特徴とする通信機器認証方法。

【請求項 1 1】 請求項 7 に記載の通信機器認証方法において、

前記サーバ装置により生成された第 2 のキー情報を認証する第 3 の認証工程を、前記サーバ装置とは別のサーバ装置にて実行することを特徴とする通信機器認証方法。

【請求項 1 2】 請求項 7 または 1 1 に記載の通信機器認証方法において、

前記別のサーバ装置は、前記第 2 のキー情報を取得した時刻とアクセス許可残り時間に基づいて前記データに対してアクセスする時間を設定することを特徴とする通信機器認証方法。

【請求項 1 3】 通信端末装置から通信手段を介して入力されるユーザ特定情報に基づいて前記通信端末装置を使用するユーザに対して認証を行い、その認証結果に基づいて前記通信端末装置にデータを供給する通信機器認証サーバ装置であって、

前記通信端末装置から送信されるユーザ特定情報を認証し、当該ユーザ特定情報に基づいて第 1 のキー情報を生成して前記通信端末装置に送信する第 1 の認証手段と、

前記通信端末装置から送信される前記第 1 のキー情報を認証し、当該第 1 のキー情報に基づいて前記データに対してアクセスする第 2 のキー情報を生成して前記通信端末装置に送信する第 2 の認証手段と、

前記通信端末装置から前記サーバ装置への前記第 2 のキー情報に基づくアクセスを所定時間内のみ許可するアクセス許可手段と、

を備えたことを特徴とする通信機器認証サーバ装置。

【請求項 1 4】 請求項 1 3 に記載の通信機器認証サーバ装置において、

前記第 1 のキー情報がアクセスされるアクセスキーであって、前記第 2 のキー

情報がセッションキーであることを特徴とする通信機器認証サーバ装置。

【請求項 1 5】 請求項 1 3 または 1 4 に記載の通信機器認証サーバ装置において、

前記第 1 の認証手段は、前記通信端末装置とは別の通信端末装置を用いて前記ユーザ特定情報が送信された場合、当該ユーザ特定情報に基づいて生成するアクセスキーを前記アクセスキーと同一のアクセスキーとして付与することを特徴とする通信機器認証サーバ装置。

【請求項 1 6】 請求項 1 3 に記載の通信機器認証サーバ装置において、

前記通信端末装置には、予め設定された装置識別情報が入力されており、この装置識別情報を前記ユーザ特定情報とともに受信可能としたことを特徴とする通信機器認証サーバ装置。

【請求項 1 7】 請求項 1 3 に記載の通信機器認証サーバ装置において、

前記生成された第 2 のキー情報を認証する第 3 の認証手段を、別のサーバ装置に設けたことを特徴とする通信機器認証サーバ装置。

【請求項 1 8】 請求項 1 3 または 1 7 に記載の通信機器認証サーバ装置において、

前記別のサーバ装置は、前記第 2 のキー情報を取得した時刻とアクセス許可残り時間に基づいて前記データに対してアクセスする時間を設定することを特徴とする通信機器認証サーバ装置。

【請求項 1 9】 通信端末装置から通信手段を介して入力されるユーザ特定情報に基づいて前記通信端末装置を使用するユーザに対して認証を行い、その認証結果に基づいてサーバ装置から前記通信端末装置にデータを供給する通信機器認証システムに含まれるコンピュータを、

前記通信端末装置から送信されるユーザ特定情報を認証し、当該ユーザ特定情報に基づいて第 1 のキー情報を生成して前記サーバ装置から前記通信端末装置に送信する第 1 の認証手段、

前記通信端末装置から送信される前記第 1 のキー情報を認証し、当該第 1 のキー情報に基づいて前記データに対してアクセスする第 2 のキー情報を生成して前記サーバ装置から前記通信端末装置に送信する第 2 の認証手段、

前記通信端末装置から前記サーバ装置への前記第 2 のキー情報に基づくアクセスを所定時間内のみ許可するアクセス許可手段、

として機能させることを特徴とする通信機器認証用プログラム。

【請求項 2 0】 請求項 1 9 に記載の通信機器認証用プログラムにおいて、前記第 1 のキー情報が前記サーバ装置に対してアクセスするアクセスキーであって、前記第 2 のキー情報がセッションキーであるように機能させることを特徴とする通信機器認証用プログラム。

【請求項 2 1】 請求項 1 9 または 2 0 に記載の通信機器認証用プログラムにおいて、

前記第 1 の認証手段として機能するコンピュータを、前記通信端末装置とは別の通信端末装置を用いて前記ユーザ特定情報が送信された場合、当該ユーザ特定情報に基づいて生成するアクセスキーを前記アクセスキーと同一のアクセスキーとして付与するように機能させることを特徴とする通信機器認証用プログラム。

【請求項 2 2】 請求項 1 9 に記載の通信機器認証用プログラムにおいて、前記通信端末装置には、予め設定された装置識別情報が入力されており、この装置識別情報を前記ユーザ特定情報とともに前記サーバ装置で受信可能とするように機能させることを特徴とする通信機器認証用プログラム。

【請求項 2 3】 請求項 1 9 に記載の通信機器認証用プログラムにおいて、前記サーバ装置により生成された第 2 のキー情報を認証する第 3 の認証手段として機能するコンピュータを、前記サーバ装置とは別のサーバ装置に機能させることを特徴とする通信機器認証用プログラム。

【請求項 2 4】 請求項 1 9 または 2 3 に記載の通信機器認証用プログラムにおいて、

前記別のサーバ装置は、前記第 2 のキー情報を取得した時刻とアクセス許可残り時間に基づいて前記データに対してアクセスする時間を設定するように機能させることを特徴とする通信機器認証用プログラム。

【請求項 2 5】 請求項 1 9 乃至 2 4 のいずれか一項に記載の通信機器認証用プログラムが記録されていることを特徴とする情報記録媒体。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

本発明は、通信機器認証システム、通信機器認証方法、通信機器認証サーバ装置、通信機器認証用プログラムおよび情報記録媒体に係り、特に通信カーナビゲーション装置、携帯情報端末などの通信端末装置で通信を行う際にセキュリティを確保した通信機器認証システム、通信機器認証方法、通信機器認証サーバ装置、通信機器認証用プログラムおよび情報記録媒体の技術分野に関する。

【 0 0 0 2 】

【従来の技術】

一般に、パーソナルコンピュータ（以下、パソコンと略称する。）などの通信端末装置における認証方式は、フォームによって転送される文書を暗号化する技術を備えたSSL（Security Sockets Layer）に対応した通信端末装置からインターネットなどの通信手段を介して入力されるパスワードなどのユーザ特定情報に基づいて通信端末装置を使用するユーザに対してサーバ装置が認証を行い、その認証結果に基づいてサーバ装置から上記通信端末装置に各種データを供給可能な方式である。

【 0 0 0 3 】

【発明が解決しようとする課題】

しかしながら、上述した従来の認証方式では、SSLに対応した通信端末装置で認証を行っているため、セキュリティ上問題がないものの、CPUの容量が小さい通信端末装置や、SSLに対応することができない通信端末装置で認証を行う場合には、パスワードなどのユーザ特定情報が漏洩する可能性がある。そして、そのユーザ特定情報が漏洩すると、ユーザ以外の者に悪用されることがあり、ユーザにとって多大な被害を被る可能性がある。

【 0 0 0 4 】

本発明は、上記事情を考慮してなされたもので、CPUの容量が小さい通信端末装置であってもデータ転送速度を低下させることなく、不正アクセスを防止し、セキュリティを著しく向上させることのできる通信機器認証システム、通信機器認証方法、通信機器認証サーバ装置、通信機器認証用プログラムおよび情報記



録媒体を提供することを目的とする。

【 0 0 0 5 】

【課題を解決するための手段】

上記課題を解決するため、請求項 1 に記載の発明は、通信端末装置から通信手段を介して入力されるユーザ特定情報に基づいて前記通信端末装置を使用するユーザに対して認証を行い、その認証結果に基づいてサーバ装置から前記通信端末装置にデータを供給する通信機器認証システムであって、前記通信端末装置から送信されるユーザ特定情報を認証し、当該ユーザ特定情報に基づいて第 1 のキー情報を生成して前記サーバ装置から前記通信端末装置に送信する第 1 の認証手段と、前記通信端末装置から送信される前記第 1 のキー情報を認証し、当該第 1 のキー情報に基づいて前記データに対してアクセスする第 2 のキー情報を生成して前記サーバ装置から前記通信端末装置に送信する第 2 の認証手段と、前記通信端末装置から前記サーバ装置への前記第 2 のキー情報に基づくアクセスを所定時間内のみ許可するアクセス許可手段と、を備えたことを特徴とする。

【 0 0 0 6 】

請求項 1 に記載の発明によれば、通信端末装置から送信されるユーザ特定情報を認証し、当該ユーザ特定情報に基づいて第 1 のキー情報を生成してサーバ装置から通信端末装置に送信する第 1 の認証手段と、通信端末装置から送信される第 1 のキー情報を認証し、当該第 1 のキー情報に基づいてデータに対してアクセスする第 2 のキー情報を生成してサーバ装置から通信端末装置に送信する第 2 の認証手段と、通信端末装置からサーバ装置への第 2 のキー情報に基づくアクセスを所定時間内のみ許可するアクセス許可手段とを備えたことにより、データに対してアクセスするための第 2 のキー情報に有効時間を設けたことで、SSLを使用しない環境下での認証の際、パスワードの使用を極力削減し、CPUの容量が小さい通信端末装置であってもデータ転送速度を低下させることなく、サーバ装置への不正アクセスを防止し、セキュリティを著しく向上させることができる。

【 0 0 0 7 】

上記課題を解決するため、請求項 2 に記載の発明は、請求項 1 に記載の通信機器認証システムにおいて、前記第 1 のキー情報が前記サーバ装置に対してアクセ

スするアクセスキーであって、前記第 2 のキー情報がセッションキーであることを特徴とする。

## 【 0 0 0 8 】

請求項 2 に記載の発明によれば、第 1 のキー情報がサーバ装置に対してアクセスするアクセスキーであって、第 2 のキー情報がデータに対してアクセスするセッションキーであることにより、SSL を使用しない認証の際、パスワードの代替とすることができる。

## 【 0 0 0 9 】

上記課題を解決するため、請求項 3 に記載の発明は、請求項 1 または 2 に記載の通信機器認証システムにおいて、前記第 1 の認証手段は、前記通信端末装置とは別の通信端末装置を用いて前記ユーザ特定情報が送信された場合、当該ユーザ特定情報に基づいて生成するアクセスキーを前記アクセスキーと同一のアクセスキーとして付与することを特徴とする。

## 【 0 0 1 0 】

請求項 3 に記載の発明によれば、第 1 の認証手段は、前記通信端末装置とは別の通信端末装置を用いて前記ユーザ特定情報が送信された場合、当該ユーザ特定情報に基づいて生成するアクセスキーを前記アクセスキーと同一のアクセスキーとして付与することにより、同一ユーザに対して同一のアクセスキーが付与されるため、一人のユーザが同一のアクセスキーで複数の通信端末装置を用いることができる。

## 【 0 0 1 1 】

上記課題を解決するため、請求項 4 に記載の発明は、請求項 1 に記載の通信機器認証システムにおいて、前記通信端末装置には、予め設定された装置識別情報が入力されており、この装置識別情報を前記ユーザ特定情報とともに前記サーバ装置で受信可能としたことを特徴とする。

## 【 0 0 1 2 】

請求項 4 に記載の発明によれば、通信端末装置に予め設定された装置識別情報を入力しておき、この装置識別情報をユーザ特定情報とともにサーバ装置で受信可能としたことにより、サーバ装置が装置識別情報も受信することで、セキュリ

ティを一段と高めることができる。

【 0 0 1 3 】

上記課題を解決するため、請求項 5 に記載の発明は、請求項 1 に記載の通信機器認証システムにおいて、前記サーバ装置により生成された第 2 のキー情報を認証する第 3 の認証手段を、前記サーバ装置とは別のサーバ装置に設けたことを特徴とする。

【 0 0 1 4 】

請求項 5 に記載の発明によれば、第 2 のキー情報を認証する第 3 の認証手段を別のサーバ装置に設けたことにより、サーバ装置の CPU 容量を低減させることができる。

【 0 0 1 5 】

上記課題を解決するため、請求項 6 に記載の発明は、請求項 1 または 5 に記載の通信機器認証システムにおいて、前記別のサーバ装置は、前記第 2 のキー情報を取得した時刻とアクセス許可残り時間に基づいて前記データに対してアクセスする時間を設定することを特徴とする。

【 0 0 1 6 】

請求項 6 に記載の発明によれば、別のサーバ装置を用いた場合であっても、データに対するアクセス時間を正確に設定することができる。

【 0 0 1 7 】

上記課題を解決するため、請求項 7 に記載の発明は、通信端末装置から通信手段を介して入力されるユーザ特定情報に基づいて前記通信端末装置を使用するユーザに対して認証を行い、その認証結果に基づいてサーバ装置から前記通信端末装置にデータを供給する通信機器認証方法であって、前記通信端末装置から送信されるユーザ特定情報を認証し、当該ユーザ特定情報に基づいて第 1 のキー情報を生成して前記サーバ装置から前記通信端末装置に送信する第 1 の認証工程と、前記通信端末装置から送信される前記第 1 のキー情報を認証し、当該第 1 のキー情報に基づいて前記データに対してアクセスする第 2 のキー情報を生成して前記サーバ装置から前記通信端末装置に送信する第 2 の認証工程と、前記通信端末装置から前記サーバ装置への前記第 2 のキー情報に基づくアクセスを所定時間内の

み許可するアクセス許可工程と、を備えたことを特徴とする。

【 0 0 1 8 】

請求項 7 に記載の発明によれば、通信端末装置から送信されるユーザ特定情報を認証し、当該ユーザ特定情報に基づいて第 1 のキー情報を生成してサーバ装置から通信端末装置に送信する第 1 の認証工程と、通信端末装置から送信される第 1 のキー情報を認証し、当該第 1 のキー情報に基づいてデータに対してアクセスする第 2 のキー情報を生成してサーバ装置から通信端末装置に送信する第 2 の認証工程と、通信端末装置からサーバ装置への第 2 のキー情報に基づくアクセスを所定時間内のみ許可するアクセス許可工程とを備えたことにより、データに対してアクセスするための第 2 のキー情報に有効時間を設けたことで、SSL を使用しない環境下での認証の際、パスワードの使用を極力削減し、CPU の容量が小さい通信端末装置であってもデータ転送速度を低下させることなく、サーバ装置への不正アクセスを防止し、セキュリティを著しく向上させることができる。

【 0 0 1 9 】

上記課題を解決するため、請求項 8 に記載の発明は、請求項 7 に記載の通信機器認証方法において、前記第 1 のキー情報が前記サーバ装置に対してアクセスするアクセスキーであって、前記第 2 のキー情報がセッションキーであることを特徴とする。

【 0 0 2 0 】

請求項 8 に記載の発明によれば、第 1 のキー情報がサーバ装置に対してアクセスするアクセスキーであって、第 2 のキー情報がデータに対してアクセスするセッションキーであることにより、SSL を使用しない認証の際、パスワードの代替とすることができる。

【 0 0 2 1 】

上記課題を解決するため、請求項 9 に記載の発明は、請求項 7 または 8 に記載の通信機器認証方法において、前記第 1 の認証工程は、前記通信端末装置とは別の通信端末装置を用いて前記ユーザ特定情報が送信された場合、当該ユーザ特定情報に基づいて生成するアクセスキーを前記アクセスキーと同一のアクセスキーとして付与することを特徴とする。

## 【 0 0 2 2 】

請求項 9 に記載の発明によれば、第 1 の認証工程は、前記通信端末装置とは別の通信端末装置を用いて前記ユーザ特定情報が送信された場合、当該ユーザ特定情報に基づいて生成するアクセスキーを前記アクセスキーと同一のアクセスキーとして付与することにより、同一ユーザに対して同一のアクセスキーが付与されるため、一人のユーザが同一のアクセスキーで複数の通信端末装置を用いることができる。

## 【 0 0 2 3 】

上記課題を解決するため、請求項 1 0 に記載の発明は、請求項 7 に記載の通信機器認証方法において、前記通信端末装置には、予め設定された装置識別情報が入力されており、この装置識別情報を前記ユーザ特定情報とともに前記サーバ装置で受信可能としたことを特徴とする。

## 【 0 0 2 4 】

請求項 1 0 に記載の発明によれば、通信端末装置に予め設定された装置識別情報を入力しておき、この装置識別情報をユーザ特定情報とともにサーバ装置で受信可能としたことにより、サーバ装置が装置識別情報も受信することで、セキュリティを一段と高めることができる。

## 【 0 0 2 5 】

上記課題を解決するため、請求項 1 1 に記載の発明は、請求項 7 に記載の通信機器認証方法において、前記サーバ装置により生成された第 2 のキー情報を認証する第 3 の認証工程を、前記サーバ装置とは別のサーバ装置にて実行することを特徴とする。

## 【 0 0 2 6 】

請求項 1 1 に記載の発明によれば、第 2 のキー情報を認証する第 3 の認証工程を別のサーバ装置にて実行することにより、サーバ装置の CPU 容量を低減させることができる。

## 【 0 0 2 7 】

上記課題を解決するため、請求項 1 2 に記載の発明は、請求項 7 または 1 1 に記載の通信機器認証方法において、前記別のサーバ装置は、前記第 2 のキー情報

を取得した時刻とアクセス許可残り時間に基づいて前記データに対してアクセスする時間を設定することを特徴とする。

## 【 0 0 2 8 】

請求項 1 2 に記載の発明によれば、別のサーバ装置を用いた場合であっても、データに対するアクセス時間を正確に設定することができる。

## 【 0 0 2 9 】

上記課題を解決するため、請求項 1 3 に記載の発明は、通信端末装置から通信手段を介して入力されるユーザ特定情報に基づいて前記通信端末装置を使用するユーザに対して認証を行い、その認証結果に基づいて前記通信端末装置にデータを供給する通信機器認証サーバ装置であって、前記通信端末装置から送信されるユーザ特定情報を認証し、当該ユーザ特定情報に基づいて第 1 のキー情報を生成して前記通信端末装置に送信する第 1 の認証手段と、前記通信端末装置から送信される前記第 1 のキー情報を認証し、当該第 1 のキー情報に基づいて前記データに対してアクセスする第 2 のキー情報を生成して前記通信端末装置に送信する第 2 の認証手段と、前記通信端末装置から前記サーバ装置への前記第 2 のキー情報に基づくアクセスを所定時間内のみ許可するアクセス許可手段と、を備えたことを特徴とする。

## 【 0 0 3 0 】

請求項 1 3 に記載の発明によれば、通信端末装置から送信されるユーザ特定情報を認証し、当該ユーザ特定情報に基づいて第 1 のキー情報を生成して通信端末装置に送信する第 1 の認証手段と、通信端末装置から送信される第 1 のキー情報を認証し、当該第 1 のキー情報に基づいてデータに対してアクセスする第 2 のキー情報を生成して通信端末装置に送信する第 2 の認証手段と、通信端末装置からサーバ装置への第 2 のキー情報に基づくアクセスを所定時間内のみ許可するアクセス許可手段とを備えたことにより、データに対してアクセスするための第 2 のキー情報に有効時間を設けたことで、SSLを使用しない環境下での認証の際、パスワードの使用を極力削減し、CPUの容量が小さい通信端末装置であってもデータ転送速度を低下させることなく、装置への不正アクセスを防止し、セキュリティを著しく向上させることができる。

## 【 0 0 3 1 】

上記課題を解決するため、請求項 1 4 に記載の発明は、請求項 1 3 に記載の通信機器認証サーバ装置において、前記第 1 のキー情報がアクセスされるアクセスキーであって、前記第 2 のキー情報がセッションキーであることを特徴とする。

## 【 0 0 3 2 】

請求項 1 4 に記載の発明によれば、第 1 のキー情報がサーバ装置に対してアクセスするアクセスキーであって、第 2 のキー情報がデータに対してアクセスするセッションキーであることにより、SSL を使用しない認証の際、パスワードの代替とすることができる。

## 【 0 0 3 3 】

上記課題を解決するため、請求項 1 5 に記載の発明は、請求項 1 3 または 1 4 に記載の通信機器認証サーバ装置において、前記第 1 の認証手段は、前記通信端末装置とは別の通信端末装置を用いて前記ユーザ特定情報が送信された場合、当該ユーザ特定情報に基づいて生成するアクセスキーを前記アクセスキーと同一のアクセスキーとして付与することを特徴とする。

## 【 0 0 3 4 】

請求項 1 5 に記載の発明によれば、第 1 の認証手段は、前記通信端末装置とは別の通信端末装置を用いて前記ユーザ特定情報が送信された場合、当該ユーザ特定情報に基づいて生成するアクセスキーを前記アクセスキーと同一のアクセスキーとして付与することにより、同一ユーザに対して同一のアクセスキーが付与されるため、一人のユーザが同一のアクセスキーで複数の通信端末装置を用いることができる。

## 【 0 0 3 5 】

上記課題を解決するため、請求項 1 6 に記載の発明は、請求項 1 3 に記載の通信機器認証サーバ装置において、前記通信端末装置には、予め設定された装置識別情報が入力されており、この装置識別情報を前記ユーザ特定情報とともに受信可能としたことを特徴とする。

## 【 0 0 3 6 】

請求項 1 6 に記載の発明によれば、通信端末装置に予め設定された装置識別情

報を入力しておき、この装置識別情報をユーザ特定情報とともにサーバ装置で受信可能としたことにより、サーバ装置が装置識別情報も受信することで、セキュリティを一段と高めることができる。

## 【 0 0 3 7 】

上記課題を解決するため、請求項 1 7 に記載の発明は、請求項 1 3 に記載の通信機器認証サーバ装置において、前記生成された第 2 のキー情報を認証する第 3 の認証手段を、別のサーバ装置に設けたことを特徴とする。

## 【 0 0 3 8 】

請求項 1 7 に記載の発明によれば、第 2 のキー情報を認証する第 3 の認証手段を別のサーバ装置に設けたことにより、サーバ装置の CPU 容量を低減させることができる。

## 【 0 0 3 9 】

上記課題を解決するため、請求項 1 8 に記載の発明は、請求項 1 3 または 1 7 に記載の通信機器認証サーバ装置において、前記別のサーバ装置は、前記第 2 のキー情報を取得した時刻とアクセス許可残り時間に基づいて前記データに対してアクセスする時間を設定することを特徴とする。

## 【 0 0 4 0 】

請求項 1 8 に記載の発明によれば、別のサーバ装置を用いた場合であっても、データに対するアクセス時間を正確に設定することができる。

## 【 0 0 4 1 】

上記課題を解決するため、請求項 1 9 に記載の発明は、通信端末装置から通信手段を介して入力されるユーザ特定情報に基づいて前記通信端末装置を使用するユーザに対して認証を行い、その認証結果に基づいてサーバ装置から前記通信端末装置にデータを供給する通信機器認証システムに含まれるコンピュータを、前記通信端末装置から送信されるユーザ特定情報を認証し、当該ユーザ特定情報に基づいて第 1 のキー情報を生成して前記サーバ装置から前記通信端末装置に送信する第 1 の認証手段、前記通信端末装置から送信される前記第 1 のキー情報を認証し、当該第 1 のキー情報に基づいて前記データに対してアクセスする第 2 のキー情報を生成して前記サーバ装置から前記通信端末装置に送信する第 2 の認証手



段、前記通信端末装置から前記サーバ装置への前記第 2 のキー情報に基づくアクセスを所定時間内のみ許可するアクセス許可手段として機能させることを特徴とする。

## 【 0 0 4 2 】

請求項 1 9 に記載の発明によれば、コンピュータを、通信端末装置から送信されるユーザ特定情報を認証し、当該ユーザ特定情報に基づいて第 1 のキー情報を生成してサーバ装置から通信端末装置に送信する第 1 の認証手段、通信端末装置から送信される第 1 のキー情報を認証し、当該第 1 のキー情報に基づいてデータに対してアクセスする第 2 のキー情報を生成してサーバ装置から通信端末装置に送信する第 2 の認証手段、通信端末装置からサーバ装置への第 2 のキー情報に基づくアクセスを所定時間内のみ許可するアクセス許可手段として機能させることにより、データに対してアクセスするための第 2 のキー情報に有効時間を設けたことで、SSL を使用しない環境下での認証の際、パスワードの使用を極力削減し、CPU の容量が小さい通信端末装置であってもデータ転送速度を低下させることなく、サーバ装置への不正アクセスを防止し、セキュリティを著しく向上させることができる。

## 【 0 0 4 3 】

上記課題を解決するため、請求項 2 0 に記載の発明は、請求項 1 9 に記載の通信機器認証用プログラムにおいて、前記第 1 のキー情報が前記サーバ装置に対してアクセスするアクセスキーであって、前記第 2 のキー情報がセッションキーであるように機能させることを特徴とする。

## 【 0 0 4 4 】

請求項 2 0 に記載の発明によれば、第 1 のキー情報がサーバ装置に対してアクセスするアクセスキーであって、第 2 のキー情報がデータに対してアクセスするセッションキーであることにより、SSL を使用しない認証の際、パスワードの代替とすることができる。

## 【 0 0 4 5 】

上記課題を解決するため、請求項 2 1 に記載の発明は、請求項 1 9 または 2 0 に記載の通信機器認証用プログラムにおいて、前記第 1 の認証手段として機能す

るコンピュータを、前記通信端末装置とは別の通信端末装置を用いて前記ユーザ特定情報が送信された場合、当該ユーザ特定情報に基づいて生成するアクセスキーを前記アクセスキーと同一のアクセスキーとして付与するように機能させることを特徴とする。

## 【 0 0 4 6 】

請求項 2 1 に記載の発明によれば、第 1 の認証手段は、前記通信端末装置とは別の通信端末装置を用いて前記ユーザ特定情報が送信された場合、当該ユーザ特定情報に基づいて生成するアクセスキーを前記アクセスキーと同一のアクセスキーとして付与することにより、同一ユーザに対して同一のアクセスキーが付与されるため、一人のユーザが同一のアクセスキーで複数の通信端末装置を用いることができる。

## 【 0 0 4 7 】

上記課題を解決するため、請求項 2 2 に記載の発明は、請求項 1 9 に記載の通信機器認証用プログラムにおいて、前記通信端末装置には、予め設定された装置識別情報が入力されており、この装置識別情報を前記ユーザ特定情報とともに前記サーバ装置で受信可能とするように機能させることを特徴とする。

## 【 0 0 4 8 】

請求項 2 2 に記載の発明によれば、通信端末装置に予め設定された装置識別情報を入力しておき、この装置識別情報をユーザ特定情報とともにサーバ装置で受信可能としたことにより、サーバ装置が装置識別情報も受信することで、セキュリティを一段と高めることができる。

## 【 0 0 4 9 】

上記課題を解決するため、請求項 2 3 に記載の発明は、請求項 1 9 に記載の通信機器認証用プログラムにおいて、前記サーバ装置により生成された第 2 のキー情報を認証する第 3 の認証手段として機能するコンピュータを、前記サーバ装置とは別のサーバ装置に機能させることを特徴とする。

## 【 0 0 5 0 】

請求項 2 3 に記載の発明によれば、第 2 のキー情報を認証する第 3 の認証手段を別のサーバ装置に設けたことにより、サーバ装置の CPU 容量を低減させるこ

とができる。

【 0 0 5 1 】

上記課題を解決するため、請求項 2 4 に記載の発明は、請求項 1 9 または 2 3 に記載の通信機器認証用プログラムにおいて、前記別のサーバ装置は、前記第 2 のキー情報を取得した時刻とアクセス許可残り時間に基づいて前記データに対してアクセスする時間を設定するように機能させることを特徴とする。

【 0 0 5 2 】

請求項 2 4 に記載の発明によれば、別のサーバ装置を用いた場合であっても、データに対するアクセス時間を正確に設定することができる。

【 0 0 5 3 】

請求項 2 5 に記載の発明は、請求項 1 9 乃至 2 4 のいずれか一項に記載の通信機器認証用プログラムが記録されていることを特徴とする。

【 0 0 5 4 】

請求項 1 9 に記載の通信機器認証用プログラムが記録されている場合には、通信端末装置から送信されるユーザ特定情報を認証し、当該ユーザ特定情報に基づいて第 1 のキー情報を生成して通信端末装置に送信する第 1 の認証手段と、通信端末装置から送信される第 1 のキー情報を認証し、当該第 1 のキー情報に基づいてデータに対してアクセスする第 2 のキー情報を生成して通信端末装置に送信する第 2 の認証手段と、通信端末装置からサーバ装置への第 2 のキー情報に基づくアクセスを所定時間内のみ許可するアクセス許可手段とを備えたことにより、データに対してアクセスするための第 2 のキー情報に有効時間を設けたことで、SSL を使用しない環境下での認証の際、パスワードの使用を極力削減し、CPU の容量が小さい通信端末装置であってもデータ転送速度を低下させることなく、装置への不正アクセスを防止し、セキュリティを著しく向上させることができる。

【 0 0 5 5 】

請求項 2 0 に記載の通信機器認証用プログラムが記録されている場合には、第 1 のキー情報がサーバ装置に対してアクセスするアクセスキーであって、第 2 のキー情報がデータに対してアクセスするセッションキーであることにより、SS

Lを使用しない認証の際、パスワードの代替とすることができる。

【 0 0 5 6 】

請求項 2 1 に記載の通信機器認証用プログラムが記録されている場合には、第 1 の認証手段は、前記通信端末装置とは別の通信端末装置を用いて前記ユーザ特定情報が送信された場合、当該ユーザ特定情報に基づいて生成するアクセスキーを前記アクセスキーと同一のアクセスキーとして付与することにより、同一ユーザに対して同一のアクセスキーが付与されるため、一人のユーザが同一のアクセスキーで複数の通信端末装置を用いることができる。

【 0 0 5 7 】

請求項 2 2 に記載の通信機器認証用プログラムが記録されている場合には、通信端末装置に予め設定された装置識別情報を入力しておき、この装置識別情報をユーザ特定情報とともにサーバ装置で受信可能としたことにより、サーバ装置が装置識別情報も受信することで、セキュリティを一段と高めることができる。

【 0 0 5 8 】

請求項 2 3 に記載の通信機器認証用プログラムが記録されている場合には、第 2 のキー情報を認証する第 3 の認証手段を別のサーバ装置に設けたことにより、サーバ装置の CPU 容量を低減させることができる。

【 0 0 5 9 】

請求項 2 4 に記載の通信機器認証用プログラムが記録されている場合には、別のサーバ装置を用いた場合であっても、データに対するアクセス時間を正確に設定することができる。

【 0 0 6 0 】

【発明の実施の形態】

以下、本発明の実施形態を図面に基づいて説明する。

【 0 0 6 1 】

なお、以下に説明する実施形態は、パソコンなどの通信端末装置から通信手段としてのインターネットを介して入力されるユーザ特定情報に基づいて車両に搭載された通信端末装置である通信カーナビゲーション装置（以下、単に通信ナビと略称する。）を使用するユーザに対して認証を行い、その認証結果に基づいて

サーバ装置から通信ナビに地図データなどのデータを供給する通信機器認証システムに対して本発明を適用した場合の実施形態である。

#### 【 0 0 6 2 】

図 1 は本発明に係る通信機器認証システムの第 1 実施形態の構成を示すブロック図、図 2 は図 1 のサーバ装置におけるデータベース部のデータ構造を示す説明図、図 3 は図 2 のデータ項目を示す説明図、図 4 は図 1 の通信端末装置であるパソコン、携帯電話機または通信カーナビゲーション装置の構成を示すブロック図、図 5 は図 4 のメモリ部に格納されるデータ構造を示す説明図である。

#### 【 0 0 6 3 】

なお、図 1 ではパソコン、携帯電話機、通信カーナビゲーション装置がそれぞれ一台の例について説明するものの、実際にはパソコン、携帯電話機、通信ナビがそれぞれ複数台存在し、これらのパソコンまたは携帯電話機がサーバ装置と通信を行うことによりユーザ特定情報が認証され、その認証結果に基づいてサーバ装置から地図データなどのデータを通信ナビで受信するシステムである。また、以下の説明では、パソコン、携帯電話機、通信ナビをまとめて通信端末装置ともいう。

#### 【 0 0 6 4 】

図 1 に示すように、本実施形態の通信機器認証システムは、通信サービス系サーバ装置（以下、単にサーバ装置と略称する。）1 と通信端末装置 2 とが通信手段としてのインターネット I N を介して互いに送受信可能であり、通信端末装置 2 がパソコン 3、携帯電話機 4 および通信ナビ 5 から構成されている。

#### 【 0 0 6 5 】

通信端末装置 2 におけるパソコン 3（または携帯電話機 4）は、ポータルサイトからメールアドレスなどのユーザデータを入力してインターネット I N を介してサーバ装置 1 に送信する一方、このサーバ装置 1 から送信される申込み番号を受信するとともに、ポータルサイトからクレジット番号を入力してインターネット I N を介してサーバ装置 1 に送信する一方、このサーバ装置 1 から送信されるユーザ I D、パスワード、ライセンス番号などのユーザアカウント（ユーザ特定情報）を受信する。

## 【 0 0 6 6 】

他方、サーバ装置 1 は、パソコン 3（または携帯電話機 4）で受信したユーザアカウントが通信ナビ 5 からインターネット I N を介して送信された場合、このユーザアカウントを認証して通信ナビ 5 に対して第 1 のキー情報としてのアクセスキーを付与するとともに、このアクセスキーおよびユーザ I D が通信ナビ 5 からインターネット I N を介して送信された場合、このアクセスキーを認証して通信ナビ 5 に対して第 2 のキー情報としてのセッションキーを付与し、このセッションキーが通信ナビ 5 からインターネット I N を介して送信された場合に通信ナビ 5 に対して必要な地図データなどを提供する。

## 【 0 0 6 7 】

次に、各構成部材の細部構成について説明する。

## 【 0 0 6 8 】

図 1 に示すように、サーバ装置 1 は、通信回線送受信部 1 1 と、第 1 および第 2 の認証手段としての認証共通部 1 2 と、セッションキーに基づくアクセスを所定時間内のみ許可するアクセス許可手段としての機能も有するシステム制御装置 1 3 と、アプリケーション部 1 4 と、ハードディスク装置などからなるデータベース部 1 5 と、を備えて構成されている。

## 【 0 0 6 9 】

上記の構成において、サーバ装置 1 の通信回線送受信部 1 1 は、インターネット I N から入力されるデータに対して予め設定されている処理を実行し、処理データとしてシステム制御装置 1 3 に出力するとともに、このシステム制御装置 1 3 から通信端末装置 2 に対して送信すべき処理データが送信されると、その処理データに対して予め設定されている処理を実行し、サーバ装置 1 のデータとしてインターネット I N を介して通信端末装置 2 へ送信する。

## 【 0 0 7 0 】

認証共通部 1 2 は、上記アクセスキー、セッションキーなどを発行するとともに、これらの管理を実行する。

## 【 0 0 7 1 】

システム制御装置 1 3 は、受信したデータまたはデータベース部 1 5 に格納さ

れたデータに基づいて各部を制御するとともに、上記セッションキーに基づくアクセスを所定時間有効とする制御を実行する。

【0072】

アプリケーション部14は、ユーザの受信したデータを解析してデータベース部15から必要なデータをシステム制御装置13が取得するように指示する。

【0073】

データベース部15は、図2および図3に示すようにユーザの氏名、住所、電話番号、メールアドレス、申込み番号、クレジットカード番号、クレジットカード有効期限、ユーザID、パスワード、ライセンス番号、アクセスキー、メーカーID、型番ID、ハードウェア番号、セッションキー、セッションキー有効時間の各データが記憶されるとともに、通信ナビ5の表示部に表示すべき地図データ、経路処理に用いられる種々のデータ、通信ナビ5の表示部に表示される地図上に示される地点の位置データおよびその地点の内容データなどを含み、ナビゲーション処理の実行に必要な地点データ、各通信ナビ5を使用しているユーザについてのデータであるユーザデータなど、ナビゲーションシステムとして実行されるナビゲーション処理に必要な全てのデータを記憶しており、これらのデータを必要に応じてシステム制御装置13に出力する。

【0074】

次に、通信端末装置2は、図4に示すように通信回線送受信部16と、システム制御部17と、データ入力部である操作部18と、表示部19と、メモリ部20と、を備えて構成されている。

【0075】

上記の構成において、通信回線送受信部16は、インターネットINから入力する端末データに対して予め設定されている入力処理を実行し、処理端末データとしてシステム制御部17に出力するとともに、このシステム制御部17からサーバ装置1に対して送信すべき処理端末データが送信されると、その処理端末データに対して予め設定されている出力処理を実行し、端末データとしてインターネットINを介してサーバ装置1へ出力する。

【0076】

システム制御部 1 7 は、受信したデータまたはメモリ部 2 0 に格納されたデータに基づいて各部を制御する。

【 0 0 7 7 】

操作部 1 8 は、表示部 1 9 に表示する地図の指定または目的地の設定などのナビゲーション処理について指定すると、その指定に対応する入力データを生成してシステム制御部 1 7 に出力する。

【 0 0 7 8 】

表示部 1 9 は、地図、地図上に示される地点の位置および経路などを表示する。

【 0 0 7 9 】

メモリ部 2 0 は、図 5 に示すようにサーバ装置 1 から送信されてきたユーザ ID、パスワード、ライセンス番号などのユーザアカウント（ユーザ特定情報）や、アクセスキー、セッションキーが記憶される他、地図データなど、一時的に記憶しておくべきデータについてシステム制御部 1 7 から出力されて一時的に記憶され、必要に応じて読み出されて表示などの処理に供される。

【 0 0 8 0 】

次に、上述した第 1 実施形態の通信機器認証システムにおいて実行される通信ナビ接続までの処理の概要を図 6 に基づいて説明する。

【 0 0 8 1 】

図 6 において、通信ナビ接続までの処理は、まずユーザによりパソコン 3 のポータルサイトからメールアドレスなどを入力して SSL を用いてサーバ装置 1 に申込み手続を実行すると、サーバ装置 1 は申込み番号を発行し、この申込み番号を電子メールによりパソコン 3 に送信する（ステップ S 1）。

【 0 0 8 2 】

次いで、パソコン 3 のポータルサイトからクレジット番号などを入力して SSL を用いてサーバ装置 1 にユーザ登録手続を実行すると、サーバ装置 1 ではユーザアカウント（ユーザ ID、パスワード、ライセンス番号）を発行し、これらのユーザアカウントは SSL を用いてパソコン 3 に送信する（ステップ S 2）。



## 【 0 0 8 3 】

なお、ステップ S 1， S 2 においては、パソコン 3 以外に携帯電話機 4 を使用してもよく、これらを持たないユーザは書面の郵送または電話による通知にてサーバ装置 1 側から上記ユーザアカウントを受信する。

## 【 0 0 8 4 】

さらに、ユーザは受信したユーザアカウント（ユーザ I D、パスワード、ライセンス番号）を通信ナビ 5 に入力してインターネット I N を介してサーバ装置 1 に簡易サインアップ用データとして送信すると、サーバ装置 1 ではユーザアカウントを認証してアクセスキーを生成し、このアクセスキーを通信ナビ 5 に送信する（ステップ S 3）。

## 【 0 0 8 5 】

そして、ユーザは受信したアクセスキーおよびユーザ I D を通信ナビ 5 に入力してインターネット I N を介してサーバ装置 1 に送信すると、サーバ装置 1 ではアクセスキーおよびユーザ I D を認証してセッションキーを生成し、このセッションキーを通信ナビ 5 に送信する（ステップ S 4）。

## 【 0 0 8 6 】

次いで、ユーザは受信したセッションキーおよびユーザ I D を通信ナビ 5 に入力してインターネット I N を介してサーバ装置 1 に送信すると、サーバ装置 1 では通信ナビ 5 に対して必要な地図データなどを提供するサービスを開始する（ステップ S 5）。

## 【 0 0 8 7 】

そして、サーバ装置 1 は、セッションキーの有効時間（例えば 5 分に設定）切れになるまで通信ナビ 5 に対して必要な地図データなどを提供し（ステップ S 5； N O）、セッションキーの有効時間に達する（ステップ S 5； Y E S）と、ステップ S 4 に戻り、ユーザは再度セッションキーを取得する。

## 【 0 0 8 8 】

次に、上述した図 6 の各ステップにおいて実行される処理の詳細を図 7 ～ 図 11 に基づいて説明する。

【 0 0 8 9 】

図 7 は図 6 のステップ S 1 の詳細を示し、ユーザ登録（申込み番号付与）処理を実行するためのフローチャートである。

【 0 0 9 0 】

図 7 に示すように、ユーザ登録（申込み番号付与）処理は、まずユーザによりパソコン 3 のポータルサイトをサーバ装置 1 側に接続すると、サーバ装置 1 側はこれを受信して接続し、ユーザはパソコン 3 の表示部 1 9 において「初めて登録する」を選択する（ステップ S 1 1 ～ S 1 4 ）。

【 0 0 9 1 】

そして、ユーザはパソコン 3 からメールアドレスや氏名などのユーザ情報を入力し、このユーザ情報をサーバ装置 1 側に S S L を用いて送信する（ステップ S 1 5, S 1 6 ）。すると、サーバ装置 1 は図 2 および図 3 に示すようなユーザ情報を受信して登録するとともに、申込み番号を発行し、この申込み番号および決済画面 URL ( U n i f o r m   R e s o u r c e   L o c a t o r ) を電子メールにてユーザのパソコン 3 に送信し、このパソコン 3 が申込み番号および決済画面 URL を受信する（ステップ S 1 7 ～ S 2 0 ）。

【 0 0 9 2 】

図 8 は図 6 のステップ S 2 の詳細を示し、ユーザ登録（ユーザアカウント付与）処理を実行するためのフローチャートである。

【 0 0 9 3 】

図 8 に示すように、ユーザ登録（ユーザアカウント付与）処理は、まずユーザによりパソコン 3 の決済画面 URL をサーバ装置 1 側に接続すると、サーバ装置 1 側はこれを受信して接続し、パソコン 3 に申込み番号入力画面を表示する（ステップ S 2 1 ～ S 2 4 ）。

【 0 0 9 4 】

そして、ユーザはパソコン 3 から申込み番号を入力し、この申込み番号情報をサーバ装置 1 側に S S L を用いて送信する（ステップ S 2 5, S 2 6 ）。すると、サーバ装置 1 は申込み番号情報を受信し、この申込み番号情報を認証した後、決済画面情報をユーザのパソコン 3 に S S L を用いて送信し、このパソコン 3 に

決済画面を表示させる（ステップ S 2 7 ～ S 2 9）。

【 0 0 9 5 】

次いで、ユーザはパソコン 3 に表示された決済画面にクレジットカード番号やカード有効期限などの必要項目を入力し、これらの情報をサーバ装置 1 側に S S L を用いて送信する（ステップ S 3 0, S 3 1）。サーバ装置 1 では、ステップ S 3 2, S 3 3 で必要項目の情報を受信した後にユーザ側に与信し、その与信が成功した場合（ステップ S 3 4 ; Y E S）には、クレジットカード番号およびカード有効期限を登録した後、ユーザアカウント（ユーザ I D、パスワード、ライセンス番号）を発行する（ステップ S 3 5, S 3 6）。一方、与信が不成功の場合（ステップ S 3 4 ; N O）には、ステップ S 3 7 でユーザ側に再入力を要求してステップ S 3 0 に戻る。

【 0 0 9 6 】

また、サーバ装置 1 は、発行されたユーザ I D、パスワード、ライセンス番号をユーザのパソコン 3 に S S L を用いて送信するとともに、電子メールでも同時に通達した後、データベース部 1 5 に上記ユーザアカウントを保存する（ステップ S 3 8, S 3 9）。

【 0 0 9 7 】

さらに、ユーザのパソコン 3 は、サーバ装置 1 から送信されてきたユーザ I D、パスワード、ライセンス番号を受信して表示部 1 9 に表示する（ステップ S 4 0, S 4 1）。

【 0 0 9 8 】

図 9 は図 6 のステップ S 3 の詳細を示し、簡易サインアップ処理を実行するためのフローチャートである。なお、上記簡易サインアップ処理は、ユーザが用いる通信ナビ 5 のハードウェア番号を取得することができない場合であって、ユーザ登録（クレジットカード番号入力）済みであることが条件である。

【 0 0 9 9 】

図 9 に示すように、簡易サインアップ処理は、まず通信ナビ 5 の表示部 1 9 に初期登録画面を表示してユーザアカウント（ユーザ I D、パスワード、ライセンス番号）を入力する（ステップ S 5 1, S 5 2）。次いで、これらユーザ I D、

パスワード、ライセンス番号を簡易サインアップ用データとして通信ナビ5に付与されているメーカID、型番IDとともに、インターネットINを介してサーバ装置1に送信する（ステップS53）。

## 【0100】

このステップS53において、SSLを使用せずにパスワードを通信回線に重畳させるのは、簡易サインアップ用データ送信時の1回のみである。この簡易サインアップ用データ送信時にパスワードを通信回線に重畳させない方法を採用する場合には、通信ナビ5およびサーバ装置1の双方で同一の暗号化の関数（ハッシュ関数）を備え、通信ナビ5で暗号化したパスワードをサーバ装置1へ送信し、サーバ装置1側で予め登録しておいたパスワードを暗号化したものと一致するか否かを判定するような方法が挙げられる。

## 【0101】

サーバ装置1は、上記簡易サインアップ用データを受信した後、サーバ装置1にユーザIDは登録されているか、ユーザIDおよびパスワードは有効か、アクセスキーは未発行かを認証する（ステップS54、S55）。認証結果がOKの場合には、ステップS56でアクセスキーを生成した後、ステップS57に進む。

## 【0102】

一方、認証結果がNGの場合には、ステップS58でエラーコードを生成した後、ステップS57に進む。なお、上記アクセスキーは生成する度に変わり、既に登録済みのユーザIDに対してアクセスキーを生成する場合（端末譲渡時など）も、異なるアクセスキーを生成する。これにより、同一ユーザアカウントを複数の通信ナビ5で使用するのを防止することができる。

## 【0103】

次に、ステップS57では、サーバ装置1から通信ナビ5にアクセスキーまたはエラーコードを送信する。通信ナビ5では、アクセスキーを受信したか否かを判断（ステップS59）し、アクセスキーを受信した場合（ステップS59；YES）には、登録確認用データとしてユーザIDおよびアクセスキーをサーバ装置1に送信する（ステップS60）。一方、アクセスキーを受信しない場合（ス

テップ S 59 ; NO) には、処理を終了する。

【0104】

ところで、サーバ装置 1 において発行したアクセスキーが何等かの障害（通信不能、圏外など）によって最悪の場合、通信ナビ 5 側に送信されない可能性もある。したがって、アクセスキーが通信ナビ 5 側に送信されなかった場合、そのユーザはサーバ接続時に簡易サインアップをやり直す必要がある。しかも、サーバ装置 1 側ではアクセスキー既存エラーを返信するため、エラー処理に手間を要することになる。そこで、ステップ S 60 において、通信ナビ 5 のアプリケーションが受信したアクセスキーをユーザ ID とともにサーバ装置 1 へ送信する。これにより、アクセスキーの受け渡しの確認が可能となる。

【0105】

サーバ装置 1 は、ステップ S 61 でアクセスキーおよびユーザ ID を受信し、アクセスキーおよびユーザ ID の有効性を照会（ステップ S 62）し、照会結果が OK の場合には、ステップ S 63 でメーカ ID、型番 ID およびアクセスキーを新規に登録した後、ステップ S 64 に進む。なお、サーバ装置 1 側では、ユーザ ID、パスワードおよびライセンス番号は、既に登録済みである。一方、照会結果が NG の場合には、ステップ S 65 でエラーコードを生成した後、ステップ S 64 に進む。

【0106】

次に、ステップ S 64 では、サーバ装置 1 から通信ナビ 5 に登録終了通知またはエラーコードを送信する一方、通信ナビ 5 では、これら登録終了通知またはエラーコードを受信してこれらを認証する（ステップ S 66）。そして、エラーコードを受信した場合（ステップ S 67 ; YES）には、処理を終了する一方、エラーコードを受信しない場合（ステップ S 67 ; NO）には、通信ナビ 5 のメモリ部 20 にユーザ ID、アクセスキーおよびライセンス番号を格納して処理を終了する（ステップ S 68）。ここで、アクセスキーはユーザに対して目視不可能な形態でメモリ部 20 に格納し、パスワードはメモリ部 20 に保存しないこととする。

【0107】

図 1 0 は図 6 のステップ S 4 の詳細を示し、セッションキー取得処理を実行するためのフローチャートである。

【 0 1 0 8 】

図 1 0 に示すように、セッションキー取得処理は、まず通信ナビ 5 からセッションキー取得用データとしてユーザ ID およびアクセスキーをサーバ装置 1 へ送信する（ステップ S 7 1）。このサーバ装置 1 は、ユーザ ID およびアクセスキーを受信（ステップ S 7 2）し、その受信したユーザ ID が登録済みか、ユーザ ID とアクセスキーとが対応するかをそれぞれ認証（ステップ S 7 3）し、ユーザ ID が登録済みであって、ユーザ ID とアクセスキーとが対応する場合（ステップ S 7 3 ; OK）には、ステップ S 7 4 で有効時間（例えば 5 分）が予め設定されたセッションキーを生成した後、セッションキーおよびその有効時間を登録する（ステップ S 7 5）。

【 0 1 0 9 】

一方、ユーザ ID が未登録であって、ユーザ ID とアクセスキーとが対応しない場合（ステップ S 7 3 ; NG）には、ステップ S 7 6 でエラーコードを生成した後、ステップ S 7 7 に進む。

【 0 1 1 0 】

次に、ステップ S 7 7 では、サーバ装置 1 から通信ナビ 5 にセッションキー、その有効時間およびエラーコードを送信する。通信ナビ 5 では、ステップ S 7 8 でこれらの情報を受信した後、セッションキーを受信したか否かを判断（ステップ S 7 9）し、セッションキーを受信した場合（ステップ S 7 9 ; YES）には、通信ナビ 5 のメモリ部 2 0 にユーザ ID、アクセスキーおよびライセンス番号とともに、セッションキー、その有効時間を格納（ステップ S 8 0）して処理を終了する。また、セッションキーを受信しない場合（ステップ S 7 9 ; NO）には、処理を終了する。

【 0 1 1 1 】

なお、これら一連の処理において、セッションキー取得時は、ユーザが通常アクセスを開始した場合、通信ナビ 5 のメモリ部 2 0 にセッションキーを格納していない場合、セッションキーエラー時、またはセッションキー有効時間超過エラ

一時のそれぞれに該当する場合には、セッションキー取得開始処理を実行する。

【 0 1 1 2 】

図 1 1 は図 6 のステップ S 5, S 6 の詳細を示し、通常アクセス認証処理を実行するためのフローチャートである。

【 0 1 1 3 】

図 1 1 に示すように、通常アクセス認証処理は、まず通信ナビ 5 からユーザ ID およびセッションキーをサーバ装置 1 に送信して通常アクセスを開始する（ステップ S 8 1）。サーバ装置 1 では、これらの情報を受信してユーザ ID は登録されているか、ユーザ ID およびセッションキーは有効かを判断するとともに、セッションキー有効時間の確認、サービス契約の確認などの認証処理を実行する（ステップ S 8 2, S 8 3）。この認証結果が OK の場合には、ステップ S 8 4 で地図データなどのサービス開始許可コードを生成する一方、認証結果が NG の場合には、ステップ S 8 5 でエラーコードを生成した後、ステップ S 8 6 に進む。

【 0 1 1 4 】

ステップ S 8 6 では、サーバ装置 1 から通信ナビ 5 にサービス開始許可コードまたはエラーコードのいずれかのコードを送信する。通信ナビ 5 では、ステップ S 8 7 でこれらサービス開始許可コードまたはエラーコードのいずれかを受信した後、エラーコードを受信したか否かを判断（ステップ S 8 8）し、エラーコードを受信しない場合（ステップ S 8 8 ; NO）には、サービス開始許可コードを受信したことになるので、サーバ装置 1 に対してサービス開始の旨の情報を送信する一方、サーバ装置 1 から地図データなどの各種コンテンツが送信される（ステップ S 8 9, S 9 0）。

【 0 1 1 5 】

また、エラーコードを受信した場合（ステップ S 8 8 ; YES）には、ステップ S 9 1 でセッションキーがエラーか否かを判断し、セッションキーがエラーの場合（ステップ S 9 1 ; YES）には、上述した図 1 0 に示すセッションキー取得処理に戻る。セッションキーがエラーでない場合（ステップ S 9 1 ; NO）には、ステップ S 9 2 でエラーに対処して処理を終了する。

## 【0116】

一方、サーバ装置1では、ダウンロードが完了したか否かを判断する（ステップS93）。すなわち、通信ナビ5に送信すべきコンテンツの送信が完了したか否かを判断し、完了しない場合（ステップS93；NO）には、ステップS94でセッションキーの有効時間（例えば5分に設定）を確認した後、上述したステップS83の照会処理に戻る。また、ダウンロードが完了した場合（ステップS93；YES）には、サーバ装置1の処理を終了する。

## 【0117】

ここで、セッションキーの有効時間は、例えば5分に設定に設定したが、これに限らず通信ナビ5に送信するデータのサイズや内容に基づいて変化させたり、延長処理したりしてもよい。

## 【0118】

また、通信ナビ5では、サーバ装置1からの地図データなどの各種コンテンツのダウンロードが完了したか否かを判断する（ステップS95）。すなわち、サーバ装置1から受信すべきコンテンツの受信が全て完了したか否かを判断し、完了しない場合（ステップS95；NO）には、上述したステップS87の受信処理に戻る。また、コンテンツの受信が完了した場合（ステップS95；YES）には、通信ナビ5の処理を終了する。

## 【0119】

以上説明したように、本実施形態の通信機器認証システムによれば、パソコン3から送信されるユーザアカウントを認証し、当該ユーザアカウントに基づいてアクセスキーを生成してサーバ装置1から通信ナビ5に送信する認証共通部12と、通信ナビ5から送信されるアクセスキーを認証し、当該アクセスキーに基づいて地図データなどに対してアクセスするセッションキーを生成してサーバ装置1から通信ナビ5に送信する認証共通部12と、通信ナビ5からサーバ装置1へのセッションキーに基づくアクセスを所定時間内のみ許可するシステム制御装置13とを備えたことにより、地図データなどにアクセスするためのセッションキーに有効時間を設けたことで、SSLを使用しない環境下での認証の際、パスワードの使用を極力削減し、CPUの容量が小さい通信端末装置2であってもデー



タ転送速度を低下させることなく、サーバ装置 1 への不正アクセスを防止し、セキュリティを著しく向上させることができる。

## 【 0 1 2 0 】

また、本実施形態によれば、第 1 のキー情報がサーバ装置に対してアクセスするアクセスキーであって、第 2 のキー情報がデータに対してアクセスするセッションキーであることにより、SSL を使用しない認証の際、パスワードの代替とすることができる。

## 【 0 1 2 1 】

さらに、本実施形態によれば、通信端末装置 5 は、通信ナビ 5、パソコン 3、携帯電話機 4、携帯情報端末のうち、選択された一種であることから、汎用性を高めることができる。

## 【 0 1 2 2 】

図 1 2 および図 1 3 は本発明に係る通信機器認証システムの第 2 実施形態における通信端末追加処理を示すフローチャート、図 1 4 (A) は第 2 実施形態において単一アクセスキー使用時のデータ構造を示す説明図、図 1 4 (B) は第 2 実施形態において 1 アクセスキーを複数の通信端末装置で使用する場合のデータ構造を示す説明図である。

## 【 0 1 2 3 】

本実施形態は、1 つのアクセスキーに対して複数台の通信端末装置を登録する場合の例を示している。具体的には、例えば一人が複数台の車両を保有し、各車両にそれぞれ通信ナビを搭載したとき、各通信ナビのアクセスキーを共通にする場合である。

## 【 0 1 2 4 】

また、本実施形態の説明では、第 1 の車両が第 1 の通信ナビを搭載し、第 2 の車両が第 2 の通信ナビを搭載しており、第 1 の通信ナビに対してユーザ ID、パスワード、ライセンス番号およびアクセスキーが既に付与され、このアクセスキーを第 2 の通信ナビに対しても登録する例について説明する。

## 【 0 1 2 5 】

図 1 2 に示すように、通信端末追加処理は、まず第 2 の通信ナビ 5 の表示部 1

9に初期登録画面を表示して第1の通信ナビ5に予め付与されているユーザアカウント（ユーザID、パスワード、ライセンス番号）を入力する（ステップS101，S102）。次いで、これらユーザID、パスワード、ライセンス番号を簡易サインアップ用データとして第2の通信ナビ5に付与されているメカID、型番IDとともにインターネットINを介してサーバ装置1に送信する（ステップS103）。

## 【0126】

サーバ装置1は、上記簡易サインアップ用データを受信した後、サーバ装置1にユーザIDは登録されているか、ユーザIDおよびパスワードは有効か、アクセスキーは未発行かをそれぞれ認証する（ステップS104，S105）。認証結果がNGの場合には、ステップS106で追加登録可能か否かを判断し、追加登録不可の場合（ステップS106；NO）には、ステップS107でエラーコードを生成した後、ステップS108に進む。

## 【0127】

ここで、ステップS106の追加登録可能か否かの判断処理は、追加登録可能な車両の台数の制限や、サービス提供者の設定によって追加登録ができない場合を考慮して設けたのであり、例えばサービス提供者の設定によって追加登録可能台数が2台まで無料で、3台目を追加しようとした場合は、ステップS106でNOとなり、既に登録済みの通信ナビ5を消去（上書き）するか、登録を断念する。なお、この場合、サービス提供者の仕様によっては、追加料金を支払うことで追加登録が可能となるようにしてもよい。

## 【0128】

ステップS108では、サーバ装置1から第2の通信ナビ5に追加登録不可であって、上書き（車両の乗換え）または追加登録する情報を送信する。ここで、1アクセスキーに対して1通信ナビしか登録することができない場合や、1アクセスキーに対して登録することのできる通信ナビ数が既に限度に達している場合には、一旦追加登録不可の案内をユーザに送信する。また、既に登録済みの通信ナビ5を消去し、新たに追加登録するか、または追加料金を支払うことにより、追加登録を可能にしてもよい。

## 【 0 1 2 9 】

一方、通信ナビ 5 は、上書きまたは追加登録する情報を受信して上書きか否かを判断する（ステップ S 1 0 9 , S 1 1 0）。上書きの場合には、サーバ装置 1 に対して登録済み端末（通信ナビ）を問い合わせする（ステップ S 1 1 1）。また、ステップ S 1 1 0 で上書きでない場合には、ステップ S 1 1 2 で追加登録するか否かを判断し、追加登録する場合（ステップ S 1 1 2 ; Y E S）には、ステップ S 1 1 3 でサーバ装置 1 に対して追加条件を問い合わせする一方、追加登録しない場合（ステップ S 1 1 2 ; N O）には、ステップ S 1 1 4 でキャンセルコードを生成する。そして、通信ナビ 5 は、これら登録済み端末（通信ナビ）問合せ情報、追加条件問合せ情報またはキャンセルコードをサーバ装置 1 に送信する（ステップ S 1 1 5）。

## 【 0 1 3 0 】

サーバ装置 1 では、それらの問い合わせ情報またはキャンセルコードを受信する（ステップ S 1 1 6）。次いで、ステップ S 1 1 7 で問合せ情報が上書きか否かを判断し、上書きの場合（ステップ S 1 1 7 ; Y E S）には、ステップ S 1 1 8 で登録済み端末（通信ナビ）を検索し、上書きでない場合（ステップ S 1 1 7 ; N O）には、ステップ S 1 1 9 で追加登録するか否かを判断し、追加登録する場合（ステップ S 1 1 9 ; Y E S）には、ステップ S 1 2 0 で追加条件を検索（参照）する。すなわち、ステップ S 1 2 0 では、端末（通信ナビ）を追加登録場合の条件（追加料金や契約内容など）を検索し、その検索結果を通信ナビ 5 側に送信する（ステップ S 1 2 1）。

## 【 0 1 3 1 】

通信ナビ 5 は、登録済み端末（通信ナビ）の検索結果および追加条件の検索結果を受信する（ステップ S 1 2 2）。そして、図 1 3 に示すように、通信ナビ 5 は、上書き処理の場合（ステップ S 1 2 3 ; Y E S）には、ステップ S 1 2 4 で上書き（消去）する端末（通信ナビ）を指定する一方、上書き処理でない場合（ステップ S 1 2 3 ; N O）には、ステップ S 1 2 5 で追加処理か否かを判断し、追加処理の場合（ステップ S 1 2 5 ; Y E S）で、追加条件が O K の場合（ステップ S 1 2 6 ; Y E S）には、追加処理コードを生成する（ステップ S 1 2 7）

。また、ステップS125で追加処理ではない場合（ステップS125；NO）や、追加条件がOKでない場合（ステップS126；NO）には、キャンセル処理を実行する（ステップS128）。

#### 【0132】

さらに、通信ナビ5は、ステップS124で指定された上書き（消去）する端末（通信ナビ）、ステップS127で生成された追加処理コードをサーバ装置1に送信する（ステップS129）。

#### 【0133】

サーバ装置1は、ステップS130で上書き（消去）する端末（通信ナビ）の情報および追加処理コードを受信し、上書き処理の場合（ステップS131；YES）には、ステップS132で指定端末（通信ナビ）無効処理を実行する一方、上書き処理でない場合（ステップS131；NO）には、ステップS133で追加処理かを判断し、追加処理の場合（ステップS133；YES）には、追加手続および処理を実行する（ステップS134）。そして、追加処理でない場合（ステップS133；NO）には、キャンセル処理を実行する（ステップS135）。

#### 【0134】

ここで、端末（通信ナビ）の追加処理登録を実行し、1ユーザIDに対して複数アクセスキーを発行する場合は、図14（A）に示すようなデータ構造となり、1アクセスキーを複数の通信ナビを所有する場合は、図14（B）に示すデータ構造となる。そして、通信ナビを追加登録した後、ユーザの通信系サービスに対する契約内容についても更新を行う。

#### 【0135】

また、サーバ装置1は、ステップS132で指定端末（通信ナビ）無効処理を実行した後、およびステップS134で追加手続および処理を実行した後は、アクセスキーを生成し、このアクセスキーまたはキャンセル処理情報を通信ナビ5に送信する（ステップS136，S137）。なお、図12に示すステップS105で認証結果がOKの場合、およびステップS106で追加登録可能な場合には、ステップS136で直接アクセスキーを生成する。

## 【0136】

一方、通信ナビ5は、ステップS138でアクセスキーまたはキャンセル処理情報を受信し、アクセスキーか否かを判断し、アクセスキーの場合（ステップS139；YES）には、登録確認用データをサーバ装置1に送信する（ステップS140）。また、アクセスキーでない場合（ステップS139；NO）には、通信ナビ5の全体の処理を終了する。

## 【0137】

サーバ装置1は、ステップS141で登録確認用データを受信し、この登録確認用データを照会し、OKの場合には該当するアクセスキーを登録する（ステップS142，S143）。また、照会結果がNGの場合にはエラーコードを生成する（ステップS144）。そして、サーバ装置1は、アクセスキーまたはエラーコードを通信ナビ5に送信する（ステップS145）。

## 【0138】

通信ナビ5は、ステップS146でアクセスキーまたはエラーコードを受信し、エラーコードの場合（ステップS147；YES）には、通信ナビ5の全体の処理を終了する。また、エラーコードでない場合（ステップS147；NO）には、アクセスキーをメモリ部20にデータとして保存する（ステップS149）。

## 【0139】

このように本実施形態によれば、同一ユーザから別の通信ナビ5を用いてユーザアカウントが送信された場合、そのユーザアカウントに基づいて生成するアクセスキーを同一のアクセスキーとして付与することにより、同一ユーザに対して同一のアクセスキーが付与されるため、一人のユーザが同一のアクセスキーで複数の通信ナビ5を用いることができる。

## 【0140】

図15は本発明に係る通信機器認証システムの第3実施形態における簡易サインアップ処理を示すフローチャートである。なお、本実施形態の簡易サインアップ処理は、ユーザが用いる通信ナビ5の装置識別情報としてのハードウェア番号を取得することができる場合であって、ユーザ登録（クレジットカード番号入力

）済みであることが条件である。

【 0 1 4 1 】

図 1 5 に示すように、簡易サインアップ処理は、まず通信ナビ 5 の表示部 1 9 に初期登録画面を表示してユーザアカウント（ユーザ I D、パスワード）を入力する（ステップ S 1 5 1、S 1 5 2）。なお、本実施形態のようにハードウェア番号を取得することができる場合には、ユーザアカウント入力時にライセンス番号が不要になる。但し、ハードウェア番号は重複しないことが前提条件である。

【 0 1 4 2 】

次いで、これらユーザ I D、パスワード、ハードウェア番号を簡易サインアップ用データとして通信ナビ 5 に付与されているメーカ I D、型番 I Dとともにインターネット I Nを介してサーバ装置 1 に送信する（ステップ S 1 5 3）。

【 0 1 4 3 】

サーバ装置 1 は、上記簡易サインアップ用データを受信した後、サーバ装置 1 にユーザ I Dは登録されているか、ユーザ I Dおよびパスワードは有効か、アクセスキーは未発行かをそれぞれ認証する（ステップ S 1 5 4、S 1 5 5）。認証結果が O K の場合には、ステップ S 1 5 6 でアクセスキーを生成した後、ステップ S 1 5 7 に進む。一方、認証結果が N G の場合には、ステップ S 1 5 8 でエラーコードを生成した後、ステップ S 1 5 7 に進む。

【 0 1 4 4 】

次に、ステップ S 1 5 7 では、サーバ装置 1 から通信ナビ 5 にアクセスキーまたはエラーコードを送信する。通信ナビ 5 では、アクセスキーを受信したか否かを判断（ステップ S 1 5 9）し、アクセスキーを受信した場合（ステップ S 1 5 9；Y E S）には、登録確認用データとしてユーザ I Dおよびアクセスキーをサーバ装置 1 に送信する（ステップ S 1 6 0）。一方、アクセスキーを受信しない場合（ステップ S 1 5 9；N O）には、処理を終了する。

【 0 1 4 5 】

サーバ装置 1 は、ステップ S 1 6 1 でアクセスキーおよびユーザ I Dを受信し、アクセスキーおよびユーザ I Dの有効性を照会（ステップ S 1 6 2）し、照会結果が O K の場合には、ステップ S 1 6 3 でハードウェア番号、メーカ I D、型

番 I D およびアクセスキーを新規に登録した後、ステップ S 1 6 4 に進む。なお、サーバ装置 1 側では、ユーザ I D およびライセンス番号などのユーザアカウントは、既に登録済みであり、ステップ S 1 6 3 でハードウェア番号（機器番号）に登録することで、通信ナビ 5 の譲渡時などに通信ナビ 5 の特定が可能となる。一方、照会結果が N G の場合には、ステップ S 1 6 5 でエラーコードを生成した後、ステップ S 1 6 4 に進む。

## 【 0 1 4 6 】

次に、ステップ S 1 6 4 では、サーバ装置 1 から通信ナビ 5 に登録終了通知またはエラーコードを送信する一方、通信ナビ 5 では、これらの登録終了通知またはエラーコードを受信してこれらを認証する（ステップ S 1 6 6）。そして、エラーコードを受信した場合（ステップ S 1 6 7；Y E S）には、処理を終了する一方、エラーコードを受信しない場合（ステップ S 1 6 7；N O）には、通信ナビ 5 のメモリ部 2 0 にユーザ I D およびアクセスキーを格納して処理を終了する（ステップ S 1 6 8）。ここで、アクセスキーはユーザに対して目視不可能な形態でメモリ部 2 0 に格納し、パスワードはメモリ部 2 0 に保存しないこととする。

## 【 0 1 4 7 】

このように本実施形態によれば、通信ナビ 5 に予め設定された装置識別情報としてのハードウェア番号を入力しておき、このハードウェア番号をメーカ I D、型番 I D、アクセスキーおよびユーザアカウントとともにサーバ装置 1 で受信可能としたことにより、サーバ装置 1 がハードウェア番号も受信することで、セキュリティを一段と高めることができる。

## 【 0 1 4 8 】

図 1 6 は本発明に係る通信機器認証システムの第 4 実施形態の構成を示すブロック図、図 1 7 は第 4 実施形態の処理を示すフローチャートである。なお、図 1 6 において図 1 と同一の構成部材には、同一の符号を付して説明する。

## 【 0 1 4 9 】

本実施形態は、サーバ装置 1 により生成された第 2 のキー情報としてのセッションキーを認証する第 3 の認証手段としての認証共通部を、サーバ装置 1 とは別

のサーバ装置としての外部ASP (Application Service Provider) 1aに設けた例である。

【0150】

外部ASP 1aは、図16に示すようにサーバ装置1と同様に通信回線送受信部11aと、サーバ装置1により生成されたセッションキーを認証する第3の認証手段としての認証共通部12aと、システム制御装置13aと、アプリケーション部14aと、ハードディスク装置などからなるデータベース部15aとを備え、インターネットINを介してサーバ装置1および通信端末装置2と送受信可能に構成されている。

【0151】

外部ASP 1aの通信回線送受信部11aは、インターネットINから入力されるプロバイダ信号に対して予め設定されている処理を実行し、処理信号としてシステム制御装置13aに出力するとともに、このシステム制御装置13aからサーバ装置1または通信端末装置2に対して送信すべき処理プロバイダ信号が出力されると、その処理プロバイダ信号に対して予め設定されている処理を実行し、プロバイダ信号としてインターネットINを介してサーバ装置1または通信端末装置2へ出力する。

【0152】

認証共通部12aは、認証キャッシュを参照することで、ユーザIDおよびセッションキーの有効を判断し、サーバ装置1により生成されたセッションキーを認証するとともに、これらの管理を実行する。

【0153】

システム制御装置13aは、受信したデータまたはデータベース部15に格納されたデータに基づいて各部を制御するとともに、上記セッションキーに基づくアクセスを所定時間有効とする制御を実行する。

【0154】

アプリケーション部14aは、受信したデータを解析してデータベース部15aから必要なデータをシステム制御装置13aが取得するように指示する。

【0155】



データベース部 1 5 a は、ユーザ I D、セッションキーおよびセッションキーの有効時間のデータ、通信ナビ 5 の表示部に表示すべき地図データ、経路処理に用いられる種々のデータ、通信ナビ 5 の表示部に表示される地図上に示される地点の位置データおよびその地点の内容データなどを含み、ナビゲーション処理の実行に必要な地点データ、各通信ナビ 5 を使用しているユーザについてのデータであるユーザデータなど、ナビゲーションシステムとして実行されるナビゲーション処理に必要な全てのデータを記憶しており、これらのデータを必要に応じてシステム制御装置 1 3 a に出力する。

## 【 0 1 5 6 】

なお、サーバ装置 1 および通信端末装置 2 の構成および機能は、前記第 1 実施形態と同様であるので、その説明を省略する。

## 【 0 1 5 7 】

次に、上述した本実施形態の通信機器認証システムにおいて実行される処理の概要を図 1 7 に基づいて説明する。なお、セッションキー取得時の処理および通常アクセス時の処理は、それぞれ図 1 0 および図 1 1 と同様である。

## 【 0 1 5 8 】

図 1 7 に示すように、本実施形態の処理は、まず通信ナビ 5 からインターネット I N を介してサーバ装置 1 にセッションキーの取得を要求する（ステップ S 1 7 1）。このサーバ装置 1 は、セッションキー取得要求の情報を受信し、有効時間（例えば 5 分）が予め設定されたセッションキーを生成する（ステップ S 1 7 2, S 1 7 3）。そして、通信ナビ 5 は、ステップ S 1 7 4 でサーバ装置 1 からセッションキー、その有効時間の情報を受信する。なお、ステップ S 1 7 3, S 1 7 4 において、セッションキーの取得を要求してきた通信ナビ 5 が依然として有効時間内のセッションキーを有している場合は、改めてセッションキーを生成しない。この場合には、通信ナビ 5 が格納しているセッションキーを継続して使用する指示の情報を送信する。

## 【 0 1 5 9 】

通信ナビ 5 は、セッションキー、その有効時間などの情報を受信した後、外部 A S P 1 a にユーザ I D およびセッションキーなどの情報を送信してサービスを

要求する（ステップ S 1 7 4， S 1 7 5）。

【 0 1 6 0 】

外部 A S P 1 a は、ステップ S 1 7 6 でユーザ I D およびセッションキーなどの情報を受信した後、ステップ S 1 7 7 に移行して認証キャッシュを参照することで、ユーザ I D およびセッションキーの有効を判断する。つまり、初めてアクセスした場合は、このステップ S 1 7 7 において N G という判断になる。そして、セッションキーが有効時間内で 2 回目以降のアクセスであれば、 O K という判断になる。

【 0 1 6 1 】

ステップ S 1 7 7 において N G の場合には、ステップ S 1 7 8 でユーザ I D、セッションキー、サービス I D および外部 A S P 1 a の I D の各情報を外部認証用データとしてサーバ装置 1 に送信する。

【 0 1 6 2 】

サーバ装置 1 は、外部認証用データを受信した後、ユーザ I D、セッションキー、サービス I D および外部 A S P 1 a の I D の各情報を認証する（ステップ S 1 7 9， S 1 8 0）。この認証判断結果が N G の場合には、ステップ S 1 8 1 でエラーコードを生成した後、ステップ S 1 8 2 に進む。認証判断結果が O K の場合には、直接ステップ S 1 8 2 に進む。このステップ S 1 8 2 では、サーバ装置 1 から外部 A S P 1 a に外部認証用データまたはエラーコードに送信する。

【 0 1 6 3 】

外部 A S P 1 a は、外部認証用データまたはエラーコードを受信した後、エラーコードか否かを判断する（ステップ S 1 8 3， S 1 8 4）。エラーコードの場合（ステップ S 1 8 4； Y E S）には、外部 A S P 1 a から通信ナビ 5 にエラーコードを送信する。この通信ナビ 5 はエラーコードを受信し、そのエラーコードがセッションキーエラーか否かを判断する（ステップ S 1 8 5， S 1 8 6）。セッションキーエラーの場合（ステップ S 1 8 6； Y E S）には、ステップ S 1 7 1 に戻り、通信ナビ 5 からサーバ装置 1 に再度セッションキー取得要求を実行する。また、セッションキーエラーでない場合（ステップ S 1 8 6； N O）には、ステップ S 1 8 7 でエラーに対処した後、後述する D L L（D y n a m i c L

ink Library) 完了の判断処理 (ステップ S182) に移行する。

【0164】

一方、ステップ S184 でエラーコードでない場合 (ステップ S184 ; NO) には、ステップ S188 でユーザ ID、セッションキー、その有効時間を外部 ASP1a に登録する。この有効時間は、セッションキー取得時刻にセッションキー許可残り時間を加えた時間となる。このように外部 ASP1a でのセッションキー有効時間は、残り時間を採用することにより、サーバ装置 1 と外部 ASP1a との時刻のずれによる影響を受けないで済むことになる。

【0165】

次いで、外部 ASP1a は、通信ナビ 5 に対してサービスを開始し、通信ナビ 5 に地図データなどの種々のコンテンツを提供する (ステップ S189, S190)。そして、外部 ASP1a では、ステップ S191 で通信ナビ 5 に送信すべきコンテンツの送信が完了したか否かを判断する。つまり、ステップ S191 では DDL が完了したか否かを判断し、完了しない場合 (ステップ S191 ; NO) には、ステップ S192 でセッションキーの有効時間を確認した後、上述したステップ S177 の認証処理に戻る。また、コンテンツの送信が完了した場合 (ステップ S191 ; YES) には、外部 ASP1a の全体の処理を終了する。

【0166】

一方、通信ナビ 5 は、ステップ S193 で受信すべき全てのコンテンツの受信が完了したか否かを判断し、コンテンツの受信が完了するまで外部 ASP1a と送受信処理 (ステップ S190) を実行し、コンテンツの受信が完了した場合 (ステップ S193 ; YES) には、通信ナビ 5 の全体の処理を終了する。

【0167】

なお、本実施形態では、外部 ASP1a がインターネット IN を介してサーバ装置 1 および通信端末装置 2 に対して送受信可能としたが、これに限らず専用回線を介して送受信可能としてもよい。

【0168】

このように本実施形態によれば、サーバ装置 1 により生成されたセッションキーを認証する認証共通部 12a を、サーバ装置 1 とは外部 ASP1a に設けたこ

とにより、サーバ装置 1 の CPU 容量を低減させることができる。

【 0 1 6 9 】

また、本実施形態によれば、外部 A S P 1 a は、セッションキーを取得した時刻とアクセス許可残り時間に基づいて地図データなどのデータに対してアクセスする時間を設定することにより、外部 A S P 1 a を用いた場合であっても、データに対するアクセス時間を正確に設定することができる。

【 0 1 7 0 】

なお、上述した各実施形態では、車両に搭載された通信端末装置 2 の通信ナビ 5 を使用するユーザに対して認証を行い、その認証結果に基づいてサーバ装置 1 から通信ナビ 5 に地図データなどのデータを供給する通信機器認証システムに対して本発明を適用した例について説明したが、これに限らずパソコン 3 や携帯電話機 4 などのように他の通信端末装置に対して認証を行い、その認証結果に基づいてサーバ装置 1 から各種データを供給する通信機器認証システムに対しても適用可能である。

【 0 1 7 1 】

また、上記各実施形態では、通信手段としてインターネット I N を用いたが、これに限らず専用回線または公衆回線などを用いた通信ネットワークを使用してよい。

【 0 1 7 2 】

さらに、上記各実施形態では、通信端末装置としてパソコン 3、携帯電話機 4 および通信ナビ 5 を用いたが、これに限らず通信機能付きの各種モバイル端末、あるいは通信機能付きの家電製品などであってもよい。

【 0 1 7 3 】

そして、上記図 1 4 および図 1 6 を除く図 6 ～図 1 7 に示したフローチャートに対するプログラムを、フレキシブルディスクまたはハードディスクなどの情報記録媒体に記録させておき、これを汎用のマイクロコンピュータなどに読み出して実行させることで、そのマイクロコンピュータを上記実施形態におけるサーバ装置 1 または外部 A S P 1 a として機能させることが可能である。

【 0 1 7 4 】

## 【発明の効果】

以上説明したように本発明によれば、通信端末装置から送信されるユーザ特定情報を認証し、当該ユーザ特定情報に基づいて第1のキー情報を生成してサーバ装置から通信端末装置に送信する第1の認証手段と、通信端末装置から送信される第1のキー情報を認証し、当該第1のキー情報に基づいてデータに対してアクセスする第2のキー情報を生成してサーバ装置から通信端末装置に送信する第2の認証手段と、通信端末装置からサーバ装置への第2のキー情報に基づくアクセスを所定時間内のみ許可するアクセス許可手段とを備えたことにより、データに対してアクセスするための第2のキー情報に有効時間を設けたことで、SSLを使用しない環境下での認証の際、パスワードの使用を極力削減し、CPUの容量が小さい通信端末装置であってもデータ転送速度を低下させることなく、サーバ装置への不正アクセスを防止し、セキュリティを著しく向上させることができる。

## 【0175】

請求項2に記載の発明によれば、請求項1に記載の効果に加えて、第1のキー情報がサーバ装置に対してアクセスするアクセスキーであって、第2のキー情報がデータに対してアクセスするセッションキーであることにより、SSLを使用しない認証の際、パスワードの代替とすることができる。

## 【0176】

請求項3に記載の発明によれば、請求項1または2に記載の効果に加えて、第1の認証手段は、前記通信端末装置とは別の通信端末装置を用いて前記ユーザ特定情報が送信された場合、当該ユーザ特定情報に基づいて生成するアクセスキーを前記アクセスキーと同一のアクセスキーとして付与することにより、同一ユーザに対して同一のアクセスキーが付与されるため、一人のユーザが同一のアクセスキーで複数の通信端末装置を用いることができる。

## 【0177】

請求項4に記載の発明によれば、請求項1に記載の効果に加えて、通信端末装置に予め設定された装置識別情報を入力しておき、この装置識別情報をユーザ特定情報とともにサーバ装置で受信可能としたことにより、サーバ装置が装置識別

情報も受信することで、セキュリティを一段と高めることができる。

【 0 1 7 8 】

請求項 5 に記載の発明によれば、請求項 1 に記載の効果に加えて、第 2 のキー情報を認証する第 3 の認証手段を別のサーバ装置に設けたことにより、サーバ装置の CPU 容量を低減させることができる。

【 0 1 7 9 】

請求項 6 に記載の発明によれば、請求項 1 または 5 に記載の効果に加えて、別のサーバ装置を用いた場合であっても、データに対するアクセス時間を正確に設定することができる。

【 0 1 8 0 】

請求項 7 に記載の発明によれば、通信端末装置から送信されるユーザ特定情報を認証し、当該ユーザ特定情報に基づいて第 1 のキー情報を生成してサーバ装置から通信端末装置に送信する第 1 の認証工程と、通信端末装置から送信される第 1 のキー情報を認証し、当該第 1 のキー情報に基づいてデータに対してアクセスする第 2 のキー情報を生成してサーバ装置から通信端末装置に送信する第 2 の認証工程と、通信端末装置からサーバ装置への第 2 のキー情報に基づくアクセスを所定時間内のみ許可するアクセス許可工程とを備えたことにより、データに対してアクセスするための第 2 のキー情報に有効時間を設けたことで、SSL を使用しない環境下での認証の際、パスワードの使用を極力削減し、CPU の容量が小さい通信端末装置であってもデータ転送速度を低下させることなく、サーバ装置への不正アクセスを防止し、セキュリティを著しく向上させることができる。

【 0 1 8 1 】

請求項 8 に記載の発明によれば、請求項 7 に記載の効果に加えて、第 1 のキー情報がサーバ装置に対してアクセスするアクセスキーであって、第 2 のキー情報がデータに対してアクセスするセッションキーであることにより、SSL を使用しない認証の際、パスワードの代替とすることができる。

【 0 1 8 2 】

請求項 9 に記載の発明によれば、請求項 7 または 8 に記載の効果に加えて、第 1 の認証工程は、同一ユーザから別の通信端末装置を用いてユーザ特定情報が送

信された場合、当該ユーザ特定情報に基づいて生成するアクセスキーを同一のアクセスキーとして付与することにより、同一ユーザに対して同一のアクセスキーが付与されるため、一人のユーザが同一のアクセスキーで複数の通信端末装置を用いることができる。

## 【 0 1 8 3 】

請求項 1 0 に記載の発明によれば、請求項 7 に記載の効果に加えて、通信端末装置に予め設定された装置識別情報を入力しておき、この装置識別情報をユーザ特定情報とともにサーバ装置で受信可能としたことにより、サーバ装置が装置識別情報も受信することで、セキュリティを一段と高めることができる。

## 【 0 1 8 4 】

請求項 1 1 に記載の発明によれば、請求項 7 に記載の効果に加えて、第 2 のキー情報を認証する第 3 の認証工程を別のサーバ装置にて実行することにより、サーバ装置の CPU 容量を低減させることができる。

## 【 0 1 8 5 】

請求項 1 2 に記載の発明によれば、請求項 7 または 1 1 に記載の効果に加えて、別のサーバ装置を用いた場合であっても、データに対するアクセス時間を正確に設定することができる。

## 【 0 1 8 6 】

請求項 1 3 に記載の発明によれば、通信端末装置から送信されるユーザ特定情報を認証し、当該ユーザ特定情報に基づいて第 1 のキー情報を生成して通信端末装置に送信する第 1 の認証手段と、通信端末装置から送信される第 1 のキー情報を認証し、当該第 1 のキー情報に基づいてデータに対してアクセスする第 2 のキー情報を生成して通信端末装置に送信する第 2 の認証手段と、通信端末装置からサーバ装置への第 2 のキー情報に基づくアクセスを所定時間内のみ許可するアクセス許可手段とを備えたことにより、データに対してアクセスするための第 2 のキー情報に有効時間を設けたことで、SSL を使用しない環境下での認証の際、パスワードの使用を極力削減し、CPU の容量が小さい通信端末装置であってもデータ転送速度を低下させることなく、装置への不正アクセスを防止し、セキュリティを著しく向上させることができる。

【 0 1 8 7 】

請求項 1 4 に記載の発明によれば、請求項 1 3 に記載の効果に加えて、第 1 のキー情報がサーバ装置に対してアクセスするアクセスキーであって、第 2 のキー情報がデータに対してアクセスするセッションキーであることにより、SSL を使用しない認証の際、パスワードの代替とすることができる。

【 0 1 8 8 】

請求項 1 5 に記載の発明によれば、請求項 1 3 または 1 4 に記載の効果に加えて、第 1 の認証手段は、前記通信端末装置とは別の通信端末装置を用いて前記ユーザ特定情報が送信された場合、当該ユーザ特定情報に基づいて生成するアクセスキーを前記アクセスキーと同一のアクセスキーとして付与することにより、同一ユーザに対して同一のアクセスキーが付与されるため、一人のユーザが同一のアクセスキーで複数の通信端末装置を用いることができる。

【 0 1 8 9 】

請求項 1 6 に記載の発明によれば、請求項 1 3 に記載の効果に加えて、通信端末装置に予め設定された装置識別情報を入力しておき、この装置識別情報をユーザ特定情報とともにサーバ装置で受信可能としたことにより、サーバ装置が装置識別情報も受信することで、セキュリティを一段と高めることができる。

【 0 1 9 0 】

請求項 1 7 に記載の発明によれば、請求項 1 3 に記載の効果に加えて、第 2 のキー情報を認証する第 3 の認証手段を別のサーバ装置に設けたことにより、サーバ装置の CPU 容量を低減させることができる。

【 0 1 9 1 】

請求項 1 8 に記載の発明によれば、請求項 1 3 または 1 7 に記載の効果に加えて、別のサーバ装置を用いた場合であっても、データに対するアクセス時間を正確に設定することができる。

【 0 1 9 2 】

請求項 1 9 に記載の発明によれば、コンピュータを、通信端末装置から送信されるユーザ特定情報を認証し、当該ユーザ特定情報に基づいて第 1 のキー情報を生成してサーバ装置から通信端末装置に送信する第 1 の認証手段、通信端末装置



から送信される第1のキー情報を認証し、当該第1のキー情報に基づいてデータに対してアクセスする第2のキー情報を生成してサーバ装置から通信端末装置に送信する第2の認証手段、通信端末装置からサーバ装置への第2のキー情報に基づくアクセスを所定時間内のみ許可するアクセス許可手段として機能させることにより、データに対してアクセスするための第2のキー情報に有効時間を設けたことで、SSLを使用しない環境下での認証の際、パスワードの使用を極力削減し、CPUの容量が小さい通信端末装置であってもデータ転送速度を低下させることなく、サーバ装置への不正アクセスを防止し、セキュリティを著しく向上させることができる。

## 【0193】

請求項20に記載の発明によれば、請求項19に記載の効果に加えて、第1のキー情報がサーバ装置に対してアクセスするアクセスキーであって、第2のキー情報がデータに対してアクセスするセッションキーであることにより、SSLを使用しない認証の際、パスワードの代替とすることができる。

## 【0194】

請求項21に記載の発明によれば、請求項19または20に記載の効果に加えて、第1の認証手段は、前記通信端末装置とは別の通信端末装置を用いて前記ユーザ特定情報が送信された場合、当該ユーザ特定情報に基づいて生成するアクセスキーを前記アクセスキーと同一のアクセスキーとして付与することにより、同一ユーザに対して同一のアクセスキーが付与されるため、一人のユーザが同一のアクセスキーで複数の通信端末装置を用いることができる。

## 【0195】

請求項22に記載の発明によれば、請求項19に記載の効果に加えて、通信端末装置に予め設定された装置識別情報を入力しておき、この装置識別情報をユーザ特定情報とともにサーバ装置で受信可能としたことにより、サーバ装置が装置識別情報も受信することで、セキュリティを一段と高めることができる。

## 【0196】

請求項23に記載の発明によれば、請求項19に記載の効果に加えて、第2のキー情報を認証する第3の認証手段を別のサーバ装置に設けたことにより、サー

バ装置のCPU容量を低減させることができる。

【0197】

請求項24に記載の発明によれば、請求項19または23に記載の効果に加えて、別のサーバ装置を用いた場合であっても、データに対するアクセス時間を正確に設定することができる。

【0198】

請求項25に記載の発明によれば、請求項19に記載の通信機器認証用プログラムが記録されている場合には、通信端末装置から送信されるユーザ特定情報を認証し、当該ユーザ特定情報に基づいて第1のキー情報を生成して通信端末装置に送信する第1の認証手段と、通信端末装置から送信される第1のキー情報を認証し、当該第1のキー情報に基づいてデータに対してアクセスする第2のキー情報を生成して通信端末装置に送信する第2の認証手段と、通信端末装置からサーバ装置への第2のキー情報に基づくアクセスを所定時間内のみ許可するアクセス許可手段とを備えたことにより、データに対してアクセスするための第2のキー情報に有効時間を設けたことで、SSLを使用しない環境下での認証の際、パスワードの使用を極力削減し、CPUの容量が小さい通信端末装置であってもデータ転送速度を低下させることなく、装置への不正アクセスを防止し、セキュリティを著しく向上させることができる。

【0199】

請求項20に記載の通信機器認証用プログラムが記録されている場合には、第1のキー情報がサーバ装置に対してアクセスするアクセスキーであって、第2のキー情報がデータに対してアクセスするセッションキーであることにより、SSLを使用しない認証の際、パスワードの代替とすることができる。

【0200】

請求項21に記載の通信機器認証用プログラムが記録されている場合には、第1の認証手段は、同一ユーザから別の通信端末装置を用いてユーザ特定情報が送信された場合、当該ユーザ特定情報に基づいて生成するアクセスキーを同一のアクセスキーとして付与することにより、同一ユーザに対して同一のアクセスキーが付与されるため、一人のユーザが同一のアクセスキーで複数の通信端末装置を

用いることができる。

【 0 2 0 1 】

請求項 2 2 に記載の通信機器認証用プログラムが記録されている場合には、通信端末装置に予め設定された装置識別情報を入力しておき、この装置識別情報をユーザ特定情報とともにサーバ装置で受信可能としたことにより、サーバ装置が装置識別情報も受信することで、セキュリティを一段と高めることができる。

【 0 2 0 2 】

請求項 2 3 に記載の通信機器認証用プログラムが記録されている場合には、第 2 のキー情報を認証する第 3 の認証手段を別のサーバ装置に設けたことにより、サーバ装置の CPU 容量を低減させることができる。

【 0 2 0 3 】

請求項 2 4 に記載の通信機器認証用プログラムが記録されている場合には、別のサーバ装置を用いた場合であっても、データに対するアクセス時間を正確に設定することができる。

【図面の簡単な説明】

【図 1】

本発明に係る通信機器認証システムの第 1 実施形態の構成を示すブロック図である。

【図 2】

図 1 のサーバ装置におけるデータベース部のデータ構造を示す説明図である。

【図 3】

図 2 のデータ項目を示す説明図である。

【図 4】

図 1 の通信端末装置であるパソコン、携帯電話機または通信カーナビゲーション装置の構成を示すブロック図である。

【図 5】

図 4 のメモリ部に格納されるデータ構造を示す説明図である。

【図 6】

第 1 実施形態の通信機器認証システムにおいて実行される通信ナビ接続までの

処理の概要を示すフローチャートである。

【図 7】

図 6 のステップ S 1 の詳細を示し、ユーザ登録（申込み番号付与）処理を実行するためのフローチャートである。

【図 8】

図 6 のステップ S 2 の詳細を示し、ユーザ登録（ユーザアカウント付与）処理を実行するためのフローチャートである。

【図 9】

図 6 のステップ S 3 の詳細を示し、簡易サインアップ処理を実行するためのフローチャートである。

【図 1 0】

図 6 のステップ S 4 の詳細を示し、セッションキー取得処理を実行するためのフローチャートである。

【図 1 1】

図 6 のステップ S 5，S 6 の詳細を示し、通常アクセス認証処理を実行するためのフローチャートである。

【図 1 2】

本発明に係る通信機器認証システムの第 2 実施形態における通信端末追加処理を示すフローチャートである。

【図 1 3】

本発明に係る通信機器認証システムの第 2 実施形態における通信端末追加処理を示すフローチャートである。

【図 1 4】

（A）は第 2 実施形態において単一アクセスキー使用時のデータ構造を示す説明図，（B）は第 2 実施形態において 1 アクセスキーを複数の通信端末装置で使用する場合のデータ構造を示す説明図である。

【図 1 5】

本発明に係る通信機器認証システムの第 3 実施形態における簡易サインアップ処理を示すフローチャートである。

【図 1 6】

本発明に係る通信機器認証システムの第 4 実施形態の構成を示すブロック図である。

【図 1 7】

第 4 実施形態の処理を示すフローチャートである。

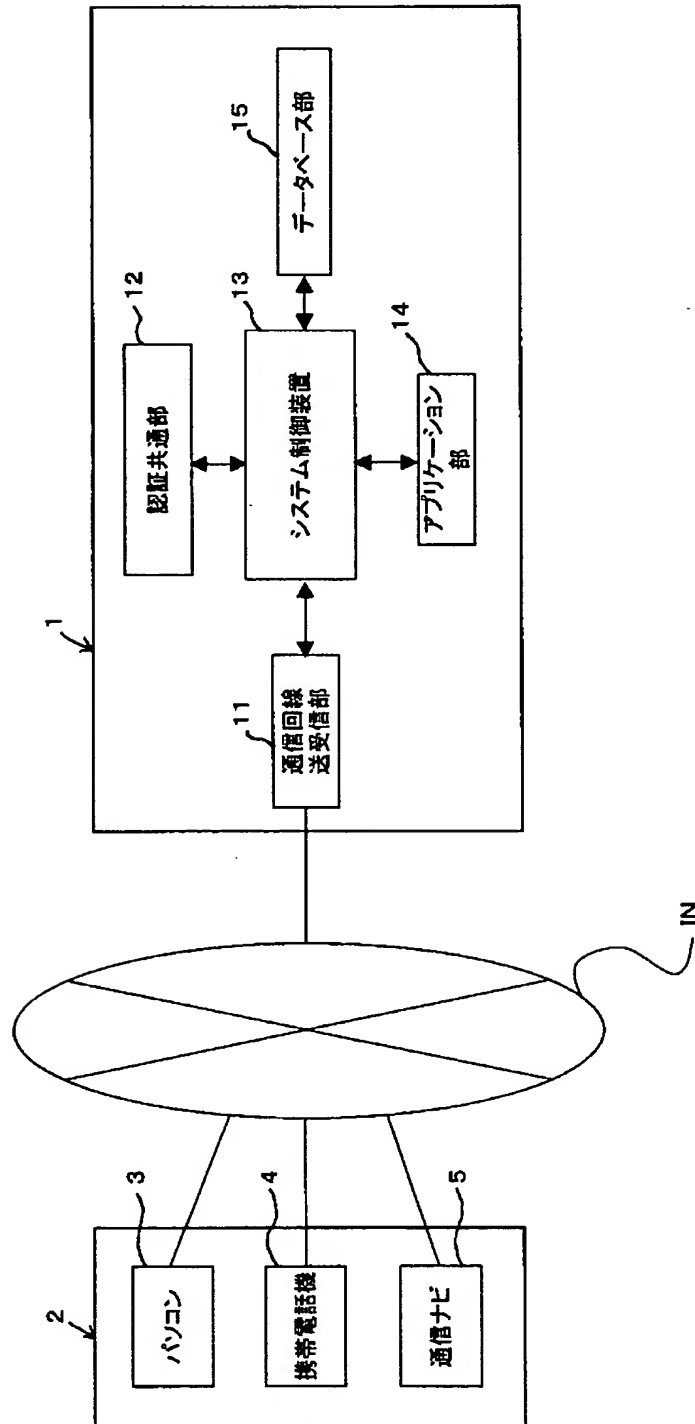
【符号の説明】

- 1 サーバ装置（通信サービス系サーバ装置）
  - 1 a 外部 A S P（別のサーバ装置）
- 2 通信端末装置
- 3 パソコン
- 4 携帯電話機
- 5 通信カーナビゲーション装置
  - 1 1 通信回線送受信部
  - 1 2 認証共通部（第 1 の認証手段、第 2 の認証手段）
    - 1 2 a 認証共通部（第 3 の認証手段）
  - 1 3 システム制御装置（アクセス許可手段）
    - 1 3 a システム制御装置
  - 1 4 アプリケーション部
    - 1 4 a アプリケーション部
  - 1 5 データベース部
    - 1 5 a データベース部
  - 1 6 通信回線送受信部
  - 1 7 システム制御部
  - 1 8 操作部
  - 1 9 表示部
  - 2 0 メモリ部
- I N インターネット（通信手段）

【書類名】

図面

【図 1】



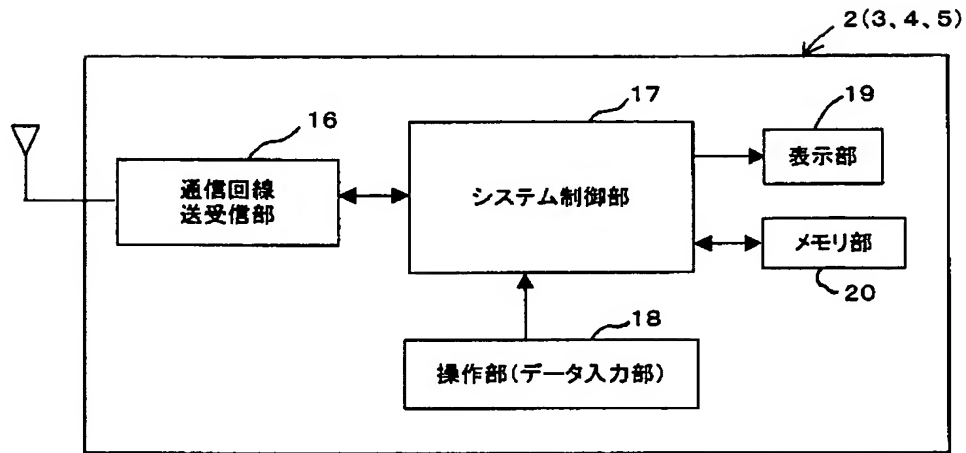
【図 2】

氏名	住所	電話 号	メールアドレス	申込みNo	クレジットカードNo
通信 太郎	東京都目黒区〇〇	03-1234-1234	mft@ipo.co.jp	200204091405	1234-1234-1234-1234
総証 太郎	東京都葛飾区〇〇	03-1233-1233	nst@ipc.co.jp	200204091406	2222-2222-2222-2222
クレジットカード有効期限	ユーザID	パスワード	ライセンス番号	アクセスキー	メーカーID
08-03	123123	456456	23217	ack0101	56788
08-03	123456	456789	22231	ack5555	56789
型番ID	ハードウェアNo	セッションキー	セッションキー有効時間		
20345687	568977	ask0023	1705		
20345687	348977	ask0056	1510		

【図 3】

データ登録項目	ユーザ登録時 必要項目	簡易サインアップ 通常アクセス時 必要項目	サーバ装置 データ登録	通信ナビ データ登録
氏名	○		○	
住所	○		○	
電話番号	○		○	
メールアドレス	○		○	
申込みNo	○		○	
クレジットカードNo	○		○	
クレジットカード有効期限	○		○	
ユーザID	○	○	○	○
パスワード	○	○	○	
ライセンス番号	○	○	○	○
アクセスキー		○	○	○
メーカーID		○	○	
型番ID		○	○	
ハードウェアNo		○	○	
セッションキー		○	○	○
セッションキー有効時間		○	○	

【図 4】

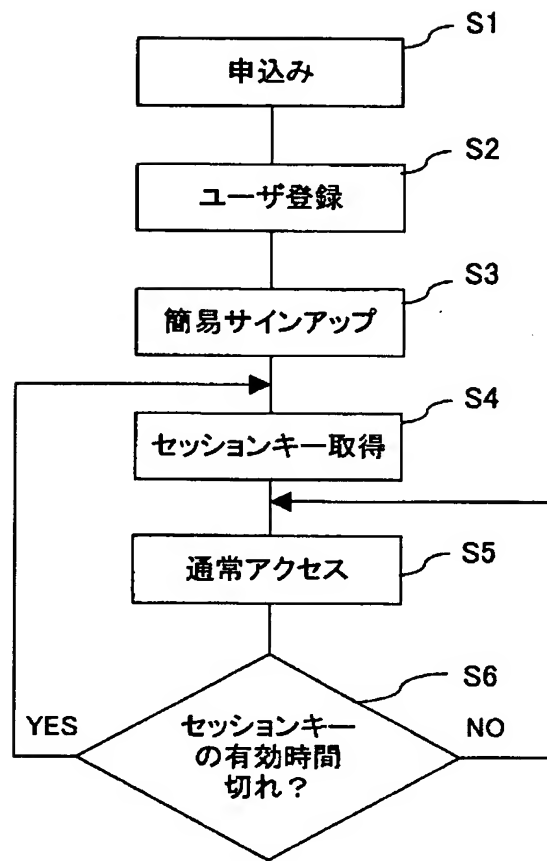


【図 5】

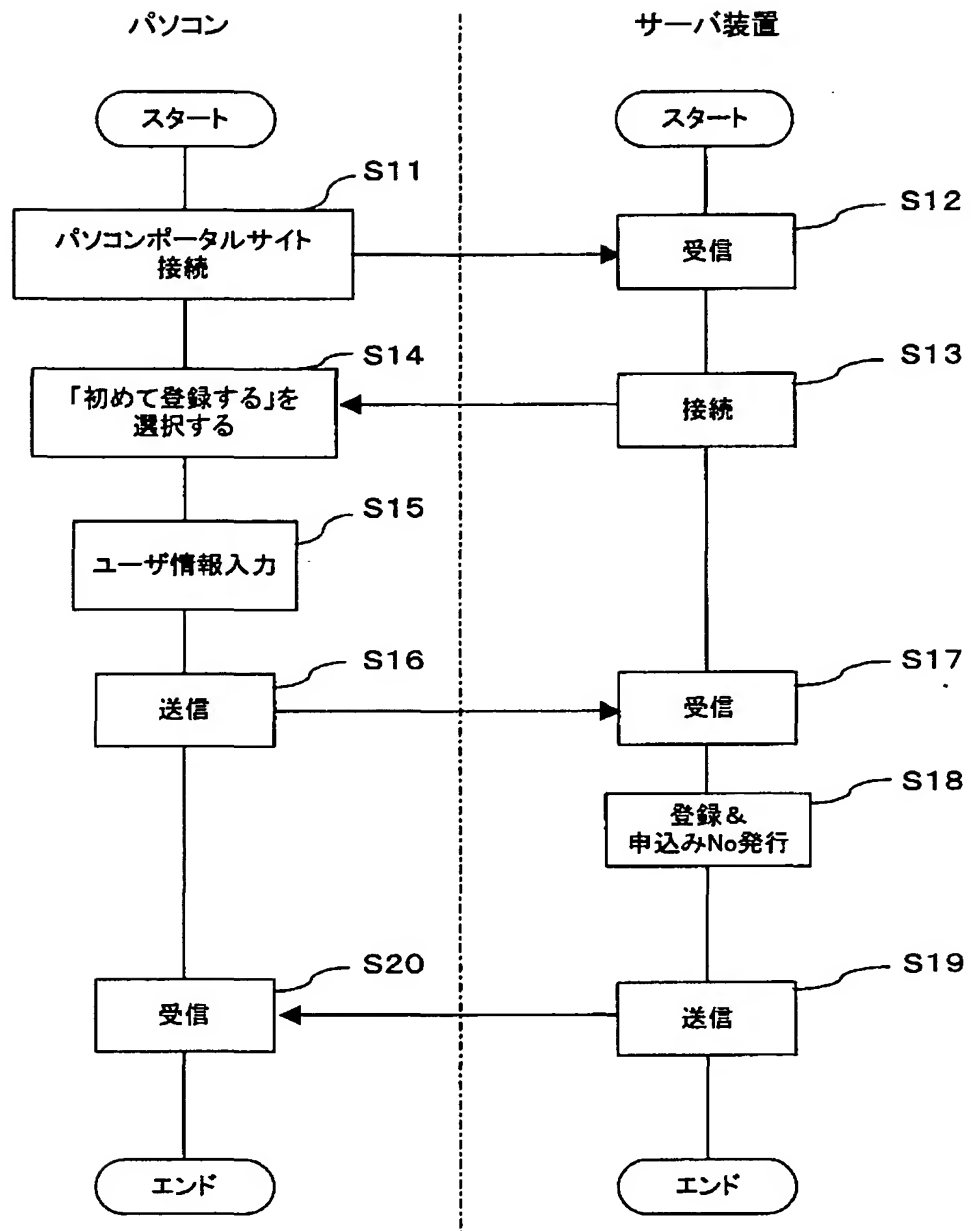
ユーザID	ライセンス 番号	アクセス キー	セッション キー
123123	23217	ack0101	ssk0023



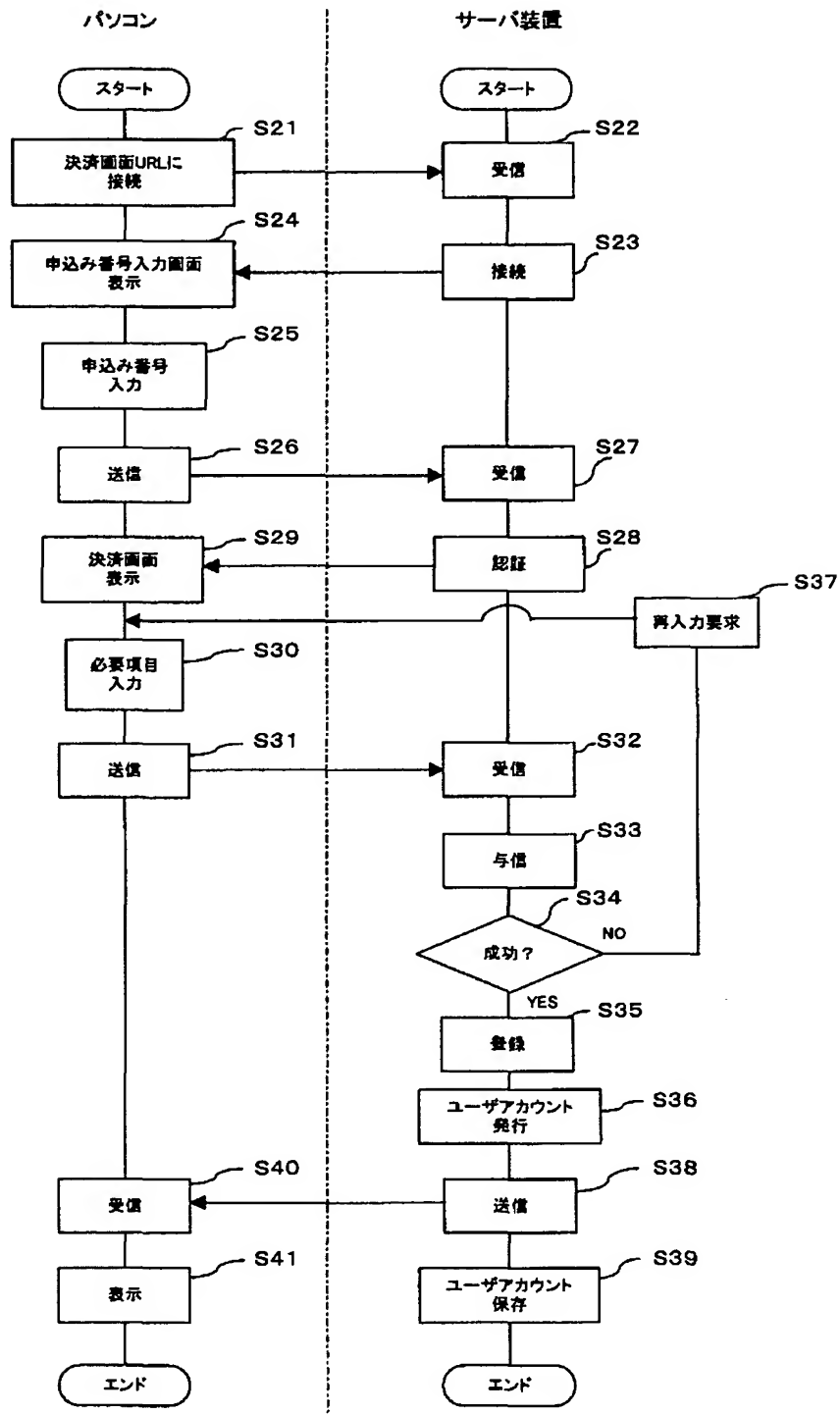
【図 6】



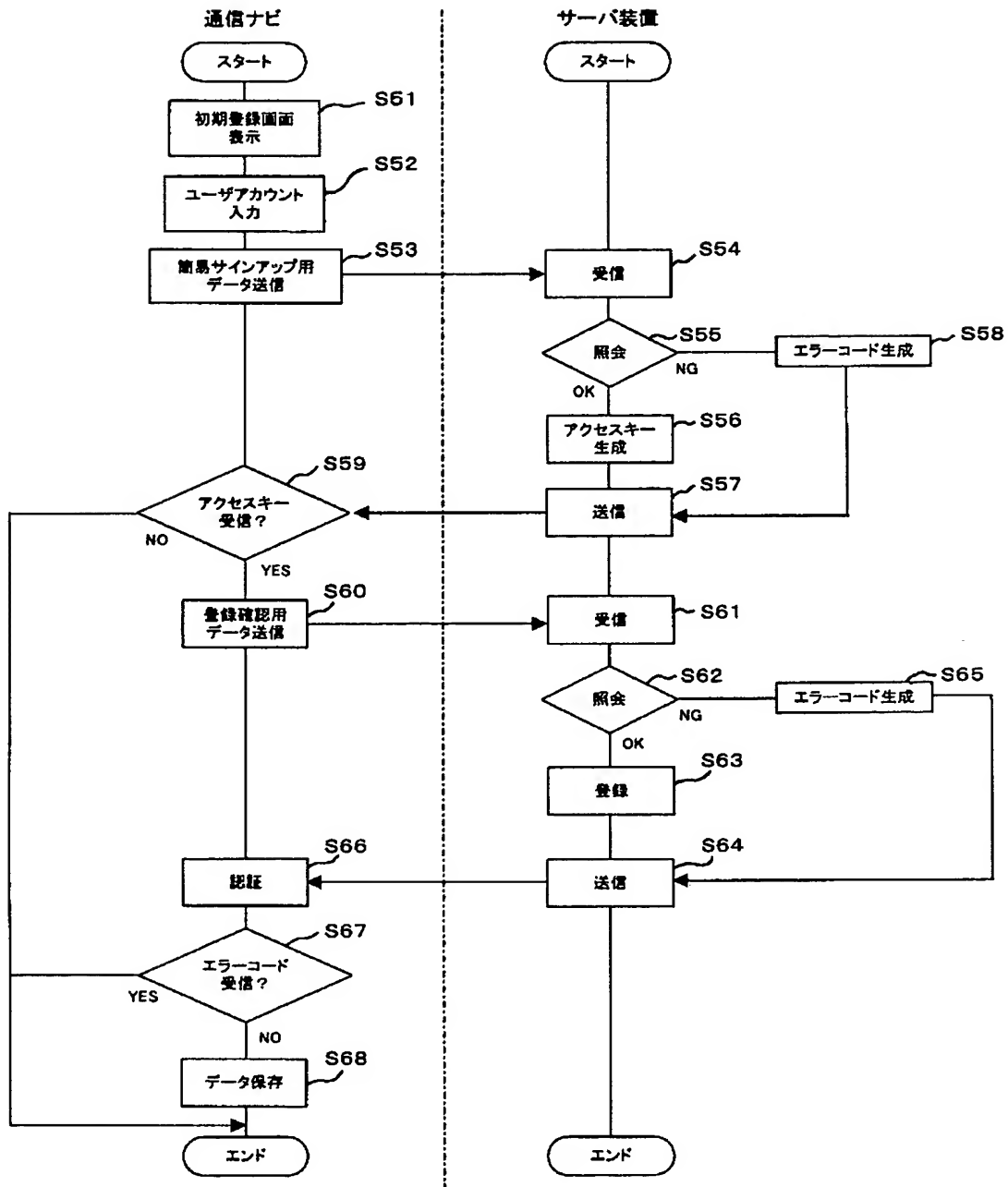
【図 7】



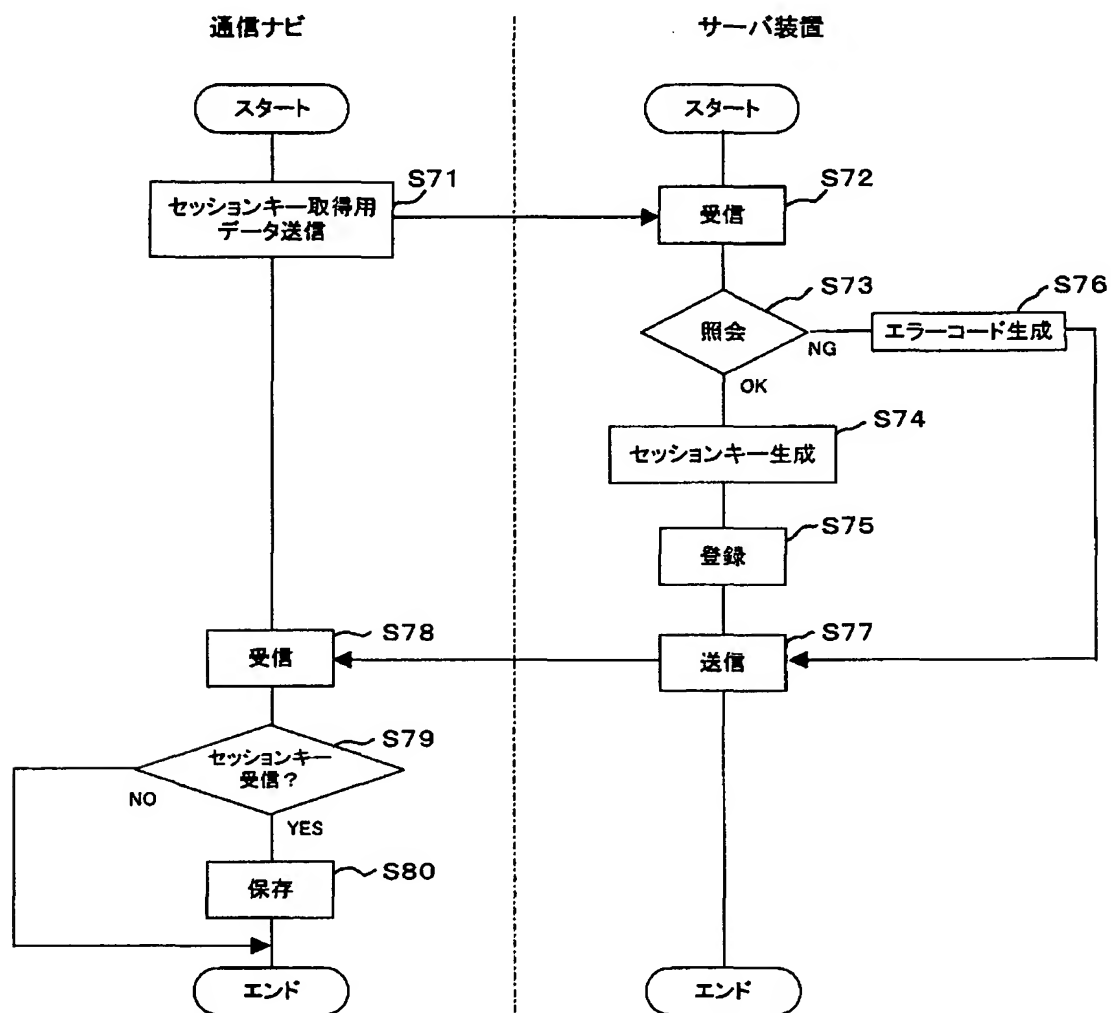
【図 8】



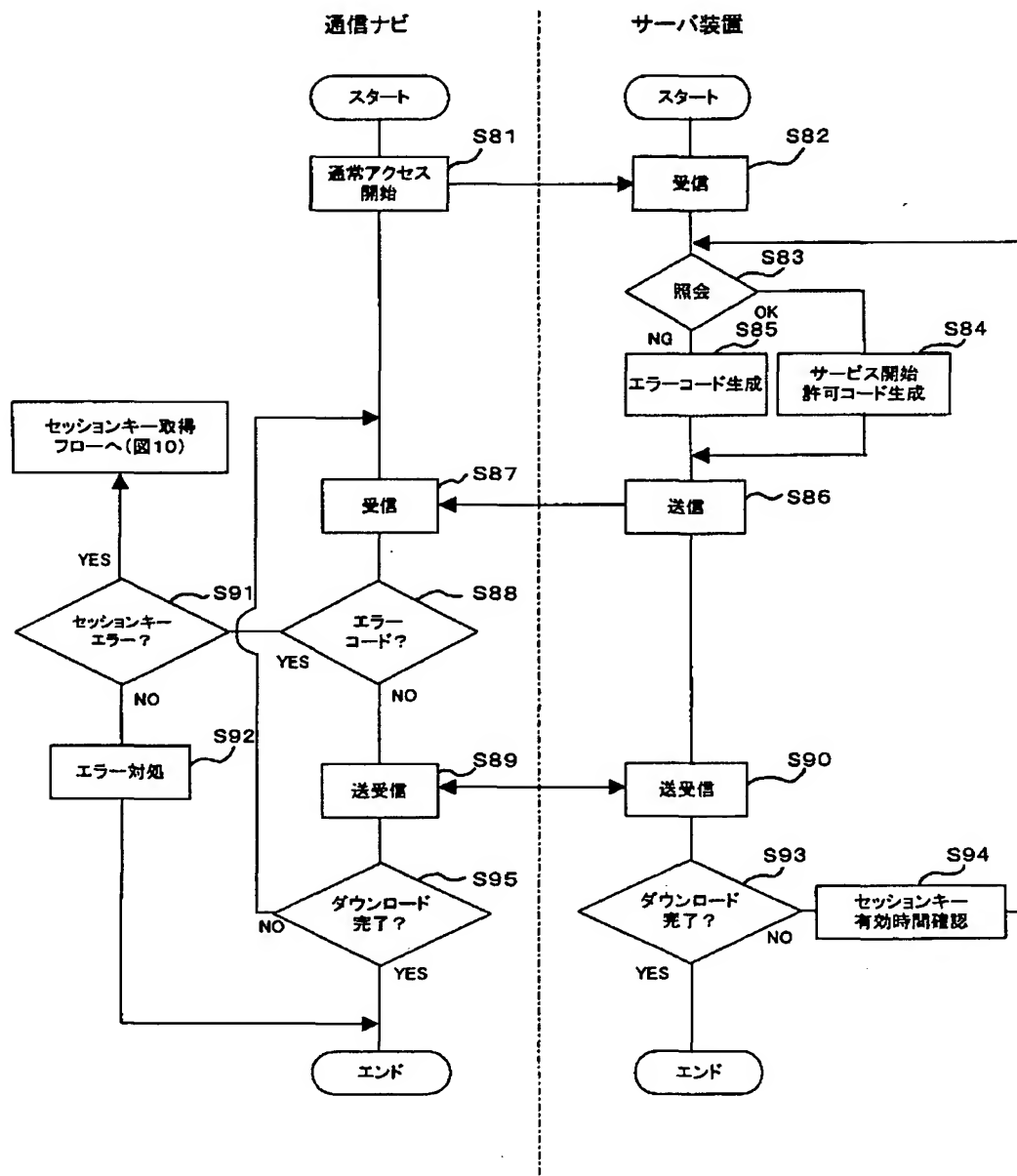
【図9】



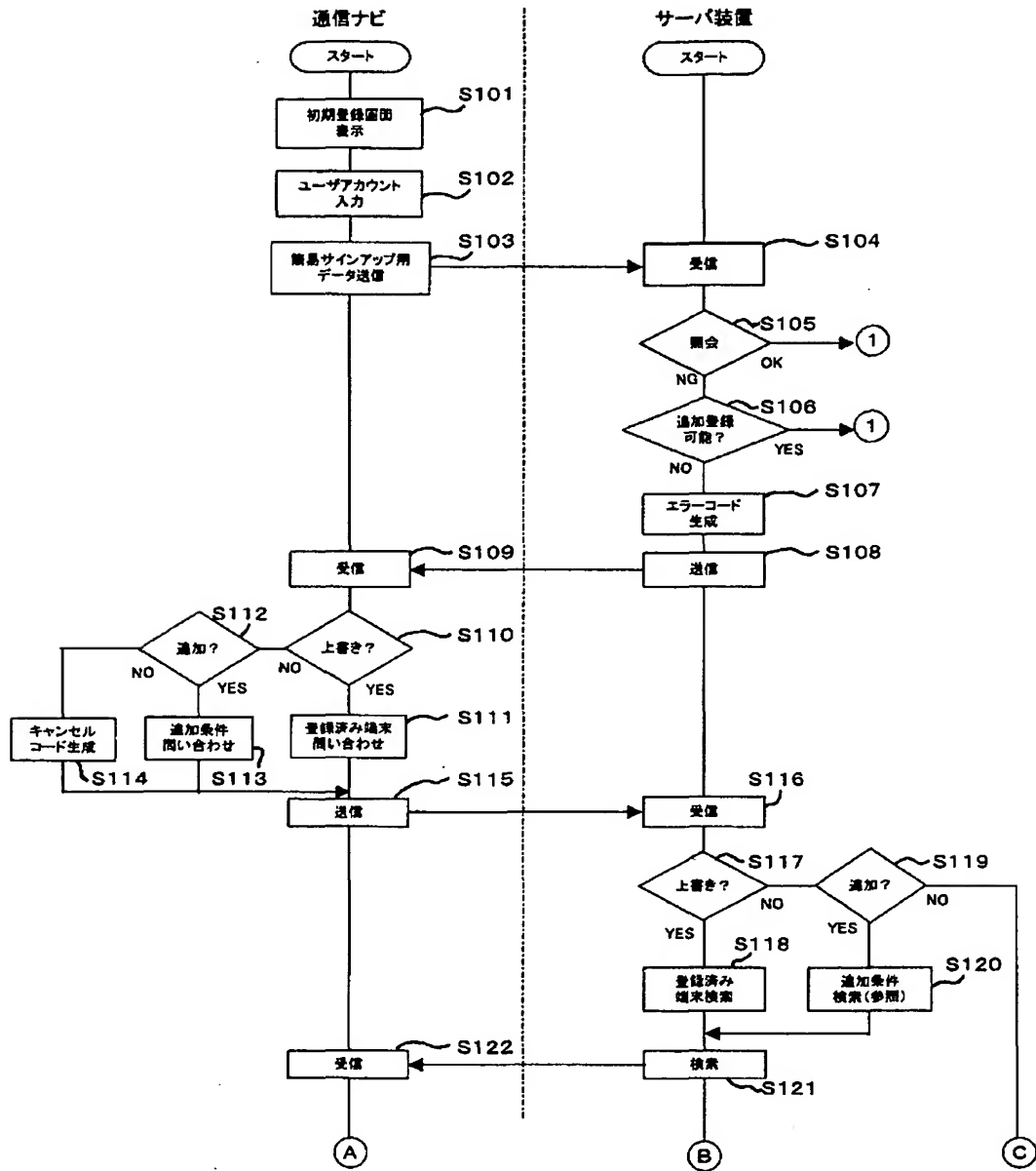
【図10】



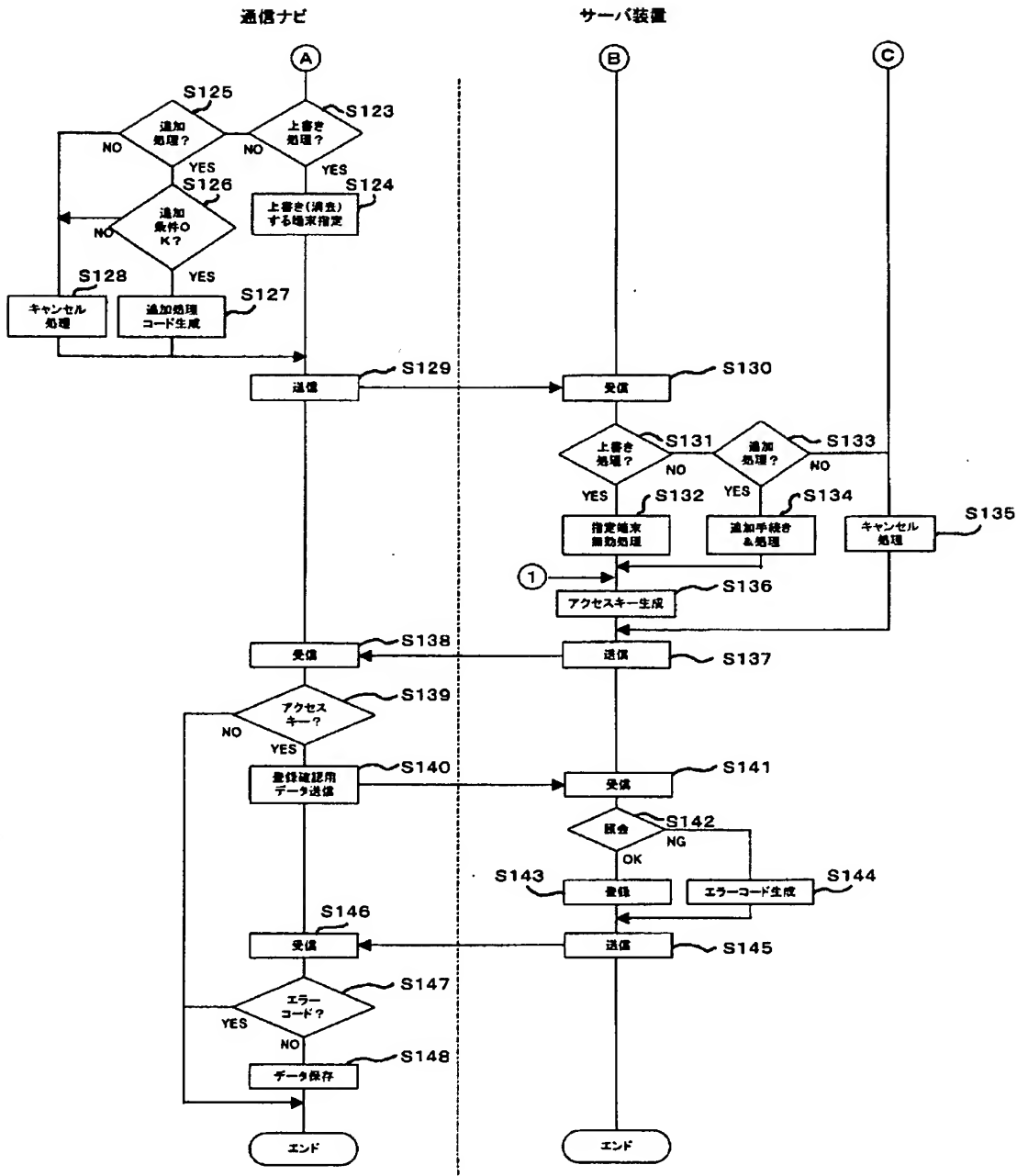
【図 11】



【図 12】



【図13】





【図 14】

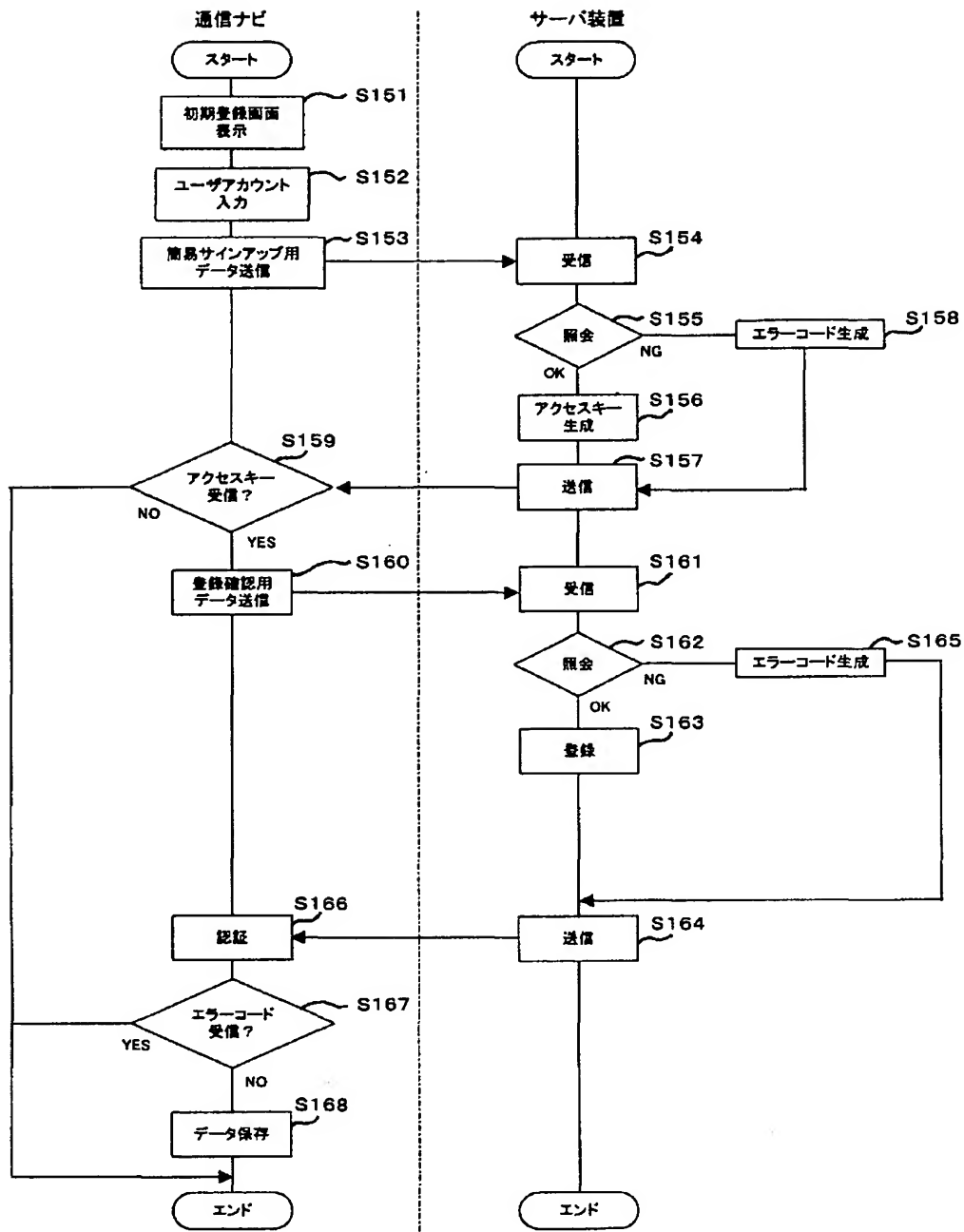
(A)

ユーザID	パスワード	アクセスキー	メーカーID	型番ID
00001	0101	ack01	P01	Y01-0001
00001	0101	ack02	P01	Y02-1234

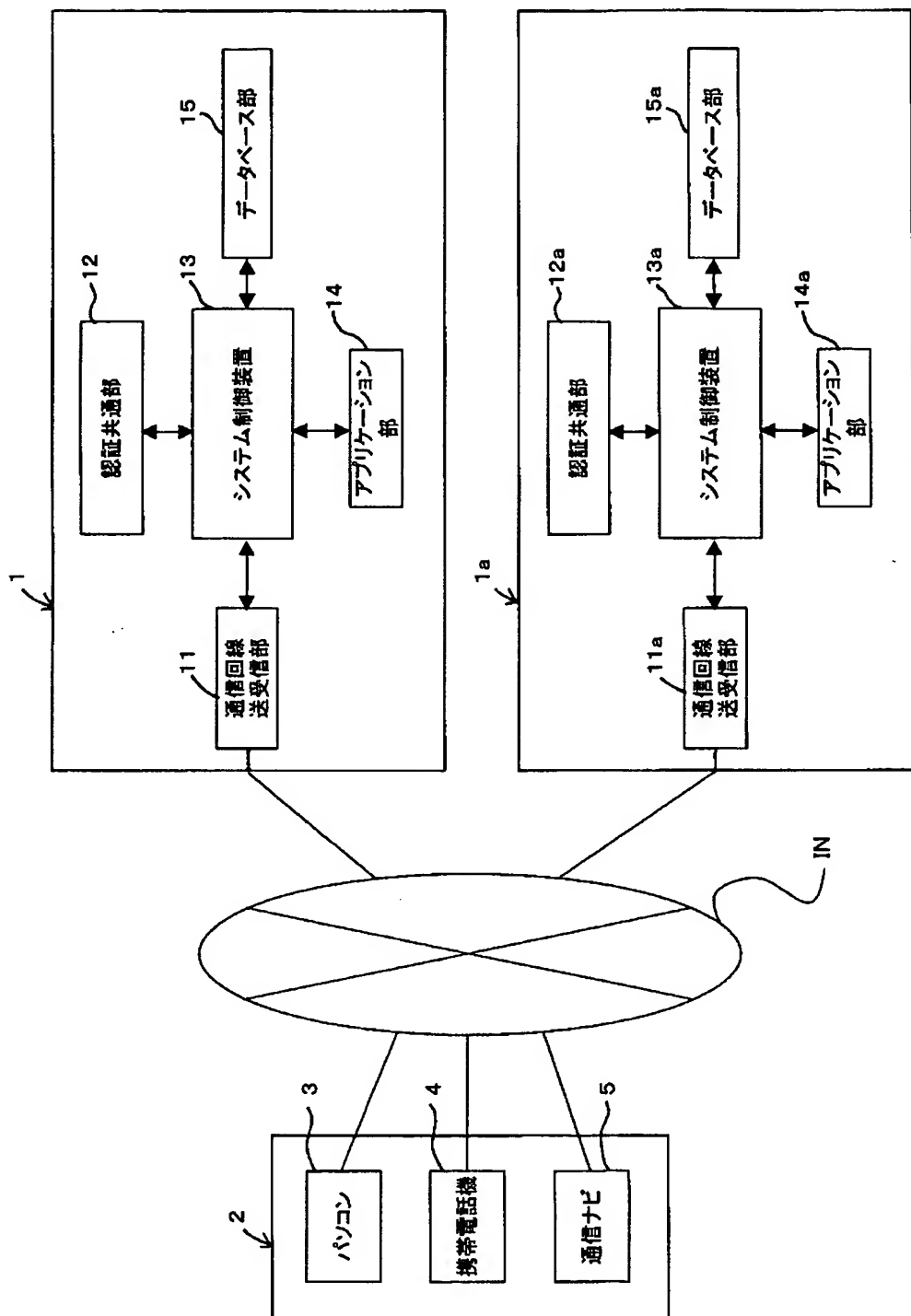
(B)

ユーザID	パスワード	アクセスキー	メーカーID	型番ID
00001	0101	ack01	P01	Y01-0001
00001	0101	ack01	P01	Y02-1234

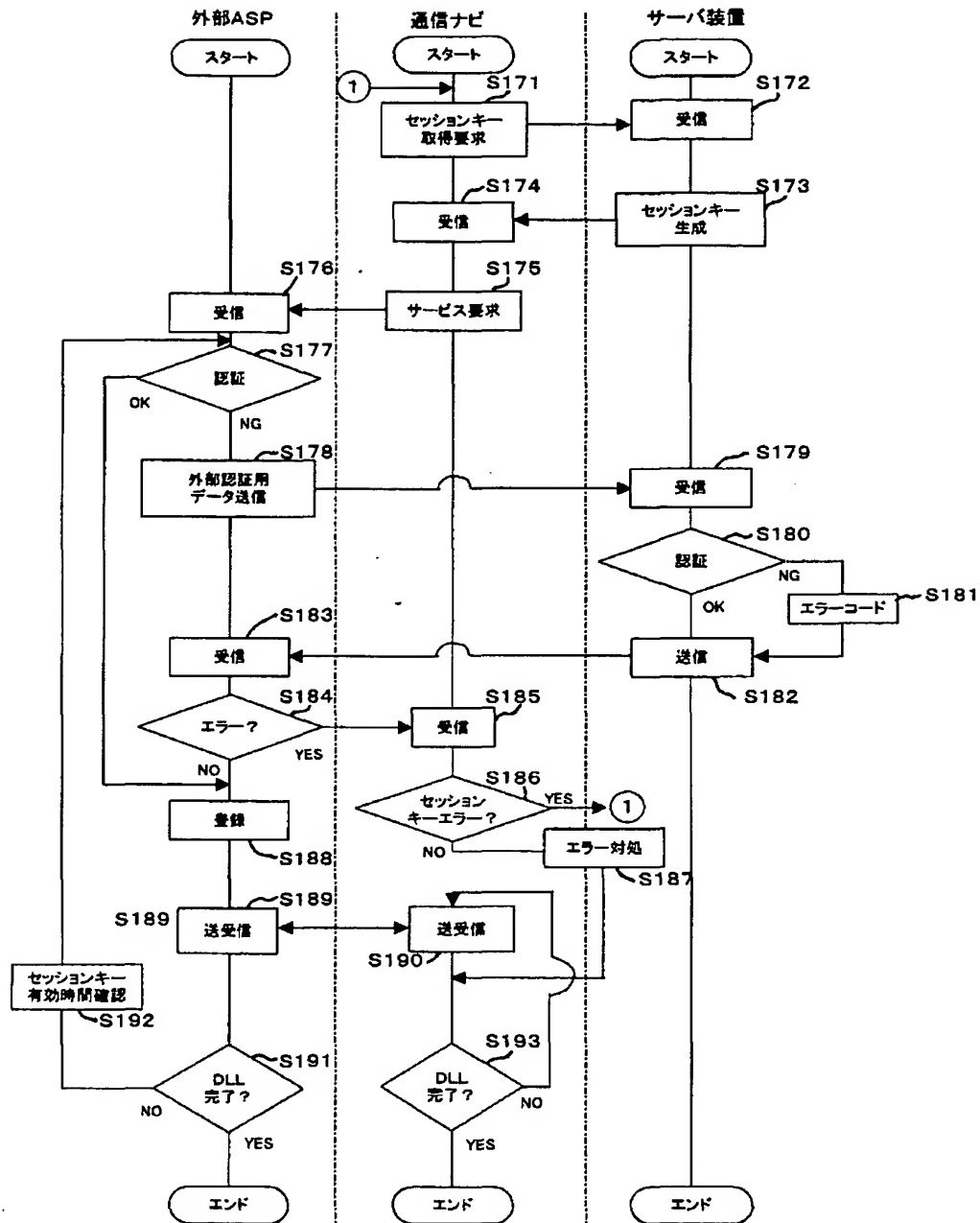
【図 15】



【図16】



【図 17】



【書類名】 要約書

【要約】

【課題】CPUの容量が小さい通信端末装置であってもデータ転送速度を低下させることなく、不正アクセスを防止し、セキュリティを著しく向上させる。

【解決手段】通信端末装置2から送信されるユーザ特定情報を認証し、当該ユーザ特定情報に基づいて第1のキー情報を生成してサーバ装置1から通信端末装置2に送信する第1の認証手段12と、通信端末装置2から送信される第1のキー情報を認証し、当該第1のキー情報に基づいてデータに対してアクセスする第2のキー情報を生成してサーバ装置1から通信端末装置2に送信する第2の認証手段12と、通信端末装置2からサーバ装置1への第2のキー情報に基づくアクセスを所定時間内のみ許可するアクセス許可手段13とを備えた。

【選択図】 図1

出 願 人 履 歴 情 報

識別番号 [595105515]

1. 変更年月日	1995年 7月21日
[変更理由]	新規登録
住 所	東京都目黒区下目黒1丁目7番1号
氏 名	インクリメント・ピー株式会社